

# HP SiteScope

for the Windows, Solaris and Linux operating systems

Software Version: 10.10

---

## Using SiteScope

Document Release Date: July 2009

Software Release Date: July 2009



# Legal Notices

## Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

## Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notices

© Copyright 2005 - 2009 Hewlett-Packard Development Company, L.P.

## Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Pentium®, and Intel® Xeon™ are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows NT®, and Windows® XP are U.S registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

**<http://h20230.www2.hp.com/selfsolve/manuals>**

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

**<http://h20229.www2.hp.com/passport-registration.html>**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

# Support

Visit the HP Software Support web site at:

**<http://www.hp.com/go/hpsoftwaresupport>**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

**<http://h20229.www2.hp.com/passport-registration.html>**

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

---

# Table of Contents

<b>Welcome to This Guide .....</b>	<b>27</b>
How This Guide Is Organized .....	27
Who Should Read This Guide .....	29
Getting More Information .....	29

## **PART I: INTRODUCTION TO SITESCOPE**

<b>Chapter 1: Introducing SiteScope.....</b>	<b>33</b>
SiteScope Overview .....	34
Key Features of SiteScope .....	35
SiteScope Architecture.....	36
SiteScope Monitoring Model.....	37
Using a Silent Login .....	38
Using the JMX Console.....	39
Access SiteScope.....	40
Create a Silent Login URL .....	42
Setup and Administration .....	45
Configure SiteScope for Monitoring – Workflow .....	48
Configure a SiteScope Monitoring Solution Using a Template – Flowchart.....	51

## **PART II: GENERAL AND ADMINISTRATION**

<b>Chapter 2: Navigating the SiteScope User Interface.....</b>	<b>55</b>
Understanding the SiteScope User Interface.....	56
Navigating and Performing Actions in the Context Tree.....	60
Performing Actions on Multiple Groups and Monitors .....	60
Copying and Moving SiteScope Objects .....	61
SiteScope Keyboard Shortcuts .....	63
Navigating SiteScope User Interface.....	64

<b>Chapter 3: Searching and Filtering SiteScope Objects.....</b>	<b>105</b>
Searching and Filtering SiteScope Objects Overview.....	105
Defining and Managing Filter Settings .....	106
Working with Search/Filter Tags.....	107
Create and Define a New Search/Filter Tag.....	108
Search/Filter Tags User Interface .....	110
<b>Chapter 4: System Availability Management Administration .....</b>	<b>119</b>
System Availability Management Administration Overview .....	120
Manage Multiple SiteScopes in System Availability Management ...	121
System Availability Management Administration User Interface ....	124
Troubleshooting and Limitations .....	146
<b>Chapter 5: Integrating with HP Business Availability Center.....</b>	<b>149</b>
Understanding SiteScope Integration with HP Business Availability Center .....	150
Configuring the Integration.....	152
Integrating SiteScope Data with HP Business Availability Center’s Configuration Items.....	155
Reporting Discovered Topologies to HP Business Availability Center .....	160
Accessing SiteScope and Building Permissions Model.....	163
Collect Data on the Performance of an IT Resource .....	164
Monitors Without Host Data .....	168
Troubleshooting and Limitations .....	170
<b>Chapter 6: Global Search and Replace .....</b>	<b>171</b>
Global Search and Replace Overview .....	171
Perform a Global Search and Replace .....	174
Global Search and Replace User Interface.....	178
<b>Chapter 7: SiteScope Tools .....</b>	<b>193</b>
SiteScope Tools Overview.....	193
Use a Tool When Configuring or Editing a Monitor .....	195
SiteScope Tools User Interface.....	196

<b>Chapter 8: Using Regular Expressions .....</b>	<b>261</b>
Regular Expressions Overview .....	262
Defining a Regular Expression .....	263
Matching String Literals .....	264
Matching Patterns with Metacharacters .....	267
Search Mode Modifiers .....	271
Retaining Content Match Values .....	273
SiteScope Date Variables.....	274
Examples for Log File Monitoring.....	279
Problems Working with Regular Expressions .....	285

### **PART III: MONITORS**

<b>Chapter 9: Working with SiteScope Groups.....</b>	<b>291</b>
SiteScope Groups Overview.....	292
Manage a Group – Workflow .....	294
SiteScope Groups User Interface.....	296
<b>Chapter 10: Working with SiteScope Monitors.....</b>	<b>301</b>
SiteScope Monitors Overview.....	302
SiteScope Monitor Categories.....	303
Monitoring Remote Servers.....	306
Monitoring Group Dependencies .....	307
Setting Status Thresholds .....	309
Setting Status Thresholds Using a Baseline.....	312
Deploy a Monitor – Workflow .....	323
Set Monitor Thresholds Using a Baseline.....	327
Monitor Categories List.....	336
Monitors Supported in Windows Environments Only.....	342
Monitors Supporting Windows Management Instrumentation (WMI) .....	343
Ports Used for SiteScope Monitoring .....	344
List of Deprecated SiteScope Monitors.....	349
SiteScope Monitors User Interface .....	350
<b>Chapter 11: Monitoring XML Documents .....</b>	<b>403</b>
Monitoring XML Documents Overview .....	403
Content Matching for XML Documents.....	404
Using XML Content Match Values in Monitor Configurations.....	406
<b>Chapter 12: Active Directory Replication Monitor .....</b>	<b>407</b>
Active Directory Replication Monitor Overview .....	407
Active Directory Replication Monitor Settings .....	409

<b>Chapter 13: Apache Server Monitor</b> .....	<b>411</b>
Apache Server Monitor Overview .....	411
Apache Server Monitor Settings .....	413
<b>Chapter 14: BroadVision Application Server Monitor</b> .....	<b>415</b>
BroadVision Application Server Monitor Overview .....	415
BroadVision Application Server Monitor Settings .....	416
<b>Chapter 15: Browsable Windows Performance Monitor</b> .....	<b>419</b>
Browsable Windows Performance Counter Monitor Overview .....	419
Browsable Windows Performance Counter Monitor Settings .....	421
<b>Chapter 16: Check Point Monitor</b> .....	<b>425</b>
Check Point Monitor Overview .....	426
Check Point Monitor Settings .....	426
<b>Chapter 17: Cisco Works Monitor</b> .....	<b>429</b>
Cisco Works Monitor Overview .....	429
Cisco Works Monitor Settings .....	430
<b>Chapter 18: Citrix Monitor</b> .....	<b>435</b>
Citrix Monitor Overview .....	435
Citrix Monitor Settings .....	439
<b>Chapter 19: ColdFusion Server Monitor</b> .....	<b>443</b>
ColdFusion Server Monitor Overview .....	443
ColdFusion Server Monitor Settings .....	445
<b>Chapter 20: COM+ Server Monitor</b> .....	<b>449</b>
COM+ Server Monitor Overview .....	450
Configure the COM+ Monitoring Environment .....	451
COM+ Server Monitor Settings .....	453
<b>Chapter 21: Composite Monitor</b> .....	<b>457</b>
Composite Monitor Overview .....	457
Composite Monitor Settings .....	458
<b>Chapter 22: CPU Monitor</b> .....	<b>461</b>
CPU Monitor Overview .....	461
CPU Monitor Settings .....	463
<b>Chapter 23: Database Counter Monitor</b> .....	<b>467</b>
Database Counter Monitor Overview .....	467
Database Counter Monitor Settings .....	471



<b>Chapter 24: Database Query Monitor .....</b>	<b>477</b>
Database Query Monitor Overview .....	477
Configure the Database Query Monitoring Environment.....	483
Database Query Monitor Settings .....	488
<b>Chapter 25: DB2 8.x and 9.x Monitor.....</b>	<b>495</b>
DB2 8.x and 9.x Monitor Overview .....	495
DB2 8.x and 9.x Monitor Settings.....	497
<b>Chapter 26: Directory Monitor .....</b>	<b>503</b>
Directory Monitor Overview .....	503
Directory Monitor Settings.....	504
<b>Chapter 27: Disk Space Monitor .....</b>	<b>509</b>
Disk Space Monitor Overview .....	509
Disk Space Monitor Settings.....	511
<b>Chapter 28: DHCP Monitor.....</b>	<b>515</b>
DHCP Monitor Overview .....	515
Configure the DHCP Monitoring Environment .....	516
DHCP Monitor Settings.....	517
<b>Chapter 29: DNS Monitor .....</b>	<b>519</b>
DNS Monitor Overview .....	519
DNS Monitor Settings.....	522
<b>Chapter 30: e-Business Transaction Monitor.....</b>	<b>525</b>
e-Business Transaction Monitor Overview.....	525
Configure the e-Business Transaction Monitoring Environment ....	528
e-Business Transaction Monitor Settings .....	530
<b>Chapter 31: F5 Big-IP Monitor .....</b>	<b>533</b>
F5 Big-IP Monitor Overview .....	533
F5 Big-IP Monitor Settings.....	534
<b>Chapter 32: File Monitor.....</b>	<b>539</b>
File Monitor Overview .....	539
File Monitor Settings .....	541
<b>Chapter 33: Formula Composite Monitor .....</b>	<b>547</b>
Formula Composite Monitor Overview .....	547
Formula Composite Monitor Settings.....	550
<b>Chapter 34: FTP Monitor.....</b>	<b>553</b>
FTP Monitor Overview .....	553
FTP Monitor Settings.....	556

<b>Chapter 35: HP NonStop Event Log Monitor .....</b>	<b>561</b>
HP NonStop Event Log Monitor Overview .....	561
HP NonStop Event Log Monitor Settings .....	562
<b>Chapter 36: HP NonStop Resources Monitor .....</b>	<b>569</b>
HP NonStop Resources Monitor Overview .....	569
HP NonStop Resources Monitor Settings .....	571
<b>Chapter 37: IPMI Monitor .....</b>	<b>573</b>
IPMI Monitor Overview .....	574
IPMI Monitor Settings .....	575
<b>Chapter 38: JMX Monitor .....</b>	<b>577</b>
JMX Monitor Overview .....	577
JMX Monitor Settings .....	582
<b>Chapter 39: LDAP Monitor .....</b>	<b>585</b>
LDAP Monitor Overview .....	585
LDAP Monitor Settings .....	587
<b>Chapter 40: Link Check Transaction Monitor .....</b>	<b>591</b>
Link Check Monitor Overview .....	591
Link Check Monitor Settings .....	592
<b>Chapter 41: Log File Monitor .....</b>	<b>597</b>
Log File Monitor Overview .....	597
Log File Monitor Settings .....	600
<b>Chapter 42: Mail Monitor .....</b>	<b>607</b>
Mail Monitor Overview .....	607
Mail Monitor Settings .....	608
<b>Chapter 43: MAPI Monitor .....</b>	<b>613</b>
MAPI Monitor Overview .....	614
Prepare the System for Using the MAPI Monitor .....	616
MAPI Monitor Settings .....	620
<b>Chapter 44: Memory Monitor .....</b>	<b>623</b>
Memory Monitor Overview .....	623
Memory Monitor Settings .....	626
<b>Chapter 45: Microsoft ASP Server Monitor .....</b>	<b>629</b>
Microsoft ASP Server Monitor Overview .....	629
Microsoft ASP Server Monitor Settings .....	631
<b>Chapter 46: Microsoft Exchange 5.5 Message Traffic Monitor .....</b>	<b>635</b>
Microsoft Exchange 5.5 Message Traffic Monitor Overview .....	636
Microsoft Exchange 5.5 Message Traffic Monitor Settings .....	637

<b>Chapter 47: Microsoft Exchange 2003 Mailbox Monitor .....</b>	<b>639</b>
Microsoft Exchange 2003 Mailbox Monitor Overview.....	640
Microsoft Exchange 2003 Mailbox Monitor Settings .....	642
<b>Chapter 48: Microsoft Exchange 2007 Monitor .....</b>	<b>645</b>
Microsoft Exchange 2007 Monitor Overview .....	645
Configure the Microsoft Exchange 2007 Monitoring Environment .....	647
Microsoft Exchange 2007 Monitor Settings.....	651
<b>Chapter 49: Microsoft Exchange 2000/2003/2007 Message Traffic Monitor .....</b>	<b>655</b>
Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Overview.....	656
Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Settings .....	658
<b>Chapter 50: Microsoft Exchange 2003 Public Folder Monitor .....</b>	<b>661</b>
Microsoft Exchange 2003 Public Folder Monitor Overview .....	662
Microsoft Exchange 2003 Public Folder Monitor Settings.....	663
<b>Chapter 51: Microsoft IIS Server Monitor .....</b>	<b>665</b>
Microsoft IIS Server Monitor Overview.....	665
Microsoft IIS Server Monitor Settings .....	668
<b>Chapter 52: Microsoft SQL Server Monitor .....</b>	<b>671</b>
Microsoft SQL Server Monitor Overview .....	672
Microsoft SQL Server Monitor Settings.....	674
<b>Chapter 53: Microsoft Windows Dial-up Monitor .....</b>	<b>679</b>
Microsoft Windows Dial-up Monitor Overview .....	679
Microsoft Windows Dial-up Monitor Settings.....	682
<b>Chapter 54: Microsoft Windows Event Log Monitor .....</b>	<b>685</b>
Microsoft Windows Event Log Monitor Overview .....	685
Microsoft Windows Event Log Monitor Settings.....	687
<b>Chapter 55: Microsoft Windows Media Player Monitor .....</b>	<b>693</b>
Microsoft Windows Media Player Monitor Overview .....	694
Microsoft Windows Media Player Monitor Settings.....	695
<b>Chapter 56: Microsoft Windows Media Server Monitor .....</b>	<b>699</b>
Microsoft Windows Media Server Monitor Overview .....	699
Microsoft Windows Media Server Monitor Settings.....	701

<b>Chapter 57: Microsoft Windows Performance Counter Monitor</b> ....	<b>705</b>
Microsoft Windows Performance Counter Monitor Overview .....	706
Microsoft Windows Performance Counter Monitor Settings .....	707
<b>Chapter 58: Microsoft Windows Resources Monitor</b> .....	<b>713</b>
Microsoft Windows Resources Monitor Overview.....	714
Configure the Microsoft Windows Resources Monitoring Environment .....	717
Microsoft Windows Resources Monitor Settings .....	720
<b>Chapter 59: Microsoft Windows Services State Monitor</b> .....	<b>725</b>
Microsoft Windows Services State Monitor Overview.....	725
Microsoft Windows Services State Monitor Settings .....	727
<b>Chapter 60: Multi Log File Monitor</b> .....	<b>731</b>
Multi Log File Monitor Overview.....	731
Multi Log Monitor Settings.....	732
<b>Chapter 61: Network Bandwidth Monitor</b> .....	<b>737</b>
Network Bandwidth Monitor Overview .....	737
Network Bandwidth Monitor Settings .....	739
<b>Chapter 62: News Monitor</b> .....	<b>745</b>
News Monitor Overview .....	745
News Monitor Settings .....	747
<b>Chapter 63: Oracle 10g Application Server Monitor</b> .....	<b>749</b>
Oracle 10g Application Server Monitor Overview .....	750
Oracle 10g Application Server Monitor Settings.....	751
<b>Chapter 64: Oracle 9i Application Server Monitor</b> .....	<b>753</b>
Oracle 9i Application Server Monitor Overview .....	753
Oracle 9i Application Server Monitor Settings .....	754
<b>Chapter 65: Oracle Database Monitor</b> .....	<b>757</b>
Oracle Database Monitor Overview .....	757
Oracle Database Monitor Settings.....	760
<b>Chapter 66: Ping Monitor</b> .....	<b>765</b>
Ping Monitor Overview .....	765
Ping Monitor Settings.....	767
<b>Chapter 67: Port Monitor</b> .....	<b>769</b>
Port Monitor Overview .....	769
Port Monitor Settings .....	771

<b>Chapter 68: Radius Monitor</b> .....	<b>773</b>
Radius Monitor Overview .....	773
Radius Monitor Settings .....	775
<b>Chapter 69: Real Media Player Monitor</b> .....	<b>777</b>
Real Media Player Monitor Overview.....	777
Real Media Player Monitor Settings .....	779
<b>Chapter 70: Real Media Server Monitor</b> .....	<b>781</b>
Real Media Server Monitor Overview.....	781
Real Media Server Monitor Settings .....	783
<b>Chapter 71: SAP CCMS Monitor</b> .....	<b>787</b>
SAP CCMS Monitor Overview .....	788
Configure the SAP CCMS Monitoring Environment.....	792
SAP CCMS Monitor Settings .....	795
<b>Chapter 72: SAP CCMS Alerts Monitor</b> .....	<b>799</b>
SAP CCMS Alerts Monitor Overview.....	800
Configure the SAP CCMS Alerts Monitoring Environment .....	801
SAP CCMS Alerts Monitor Settings .....	804
<b>Chapter 73: SAP Java Web Application Server Monitor</b> .....	<b>807</b>
SAP Java Web Application Server Monitor Overview .....	808
Configure the SAP Java Web Application Server Monitoring Environment .....	809
SAP Java Web Application Server Monitor Settings.....	811
<b>Chapter 74: SAP Performance Monitor</b> .....	<b>813</b>
SAP Performance Monitor Overview.....	814
Configure the SAP Performance Monitoring Environment .....	815
SAP Performance Monitor Settings .....	818
<b>Chapter 75: SAP Work Processes Monitor</b> .....	<b>821</b>
SAP Work Processes Monitor Overview .....	822
Configure the SAP Work Processes Monitoring Environment .....	826
SAP Work Processes Monitor Settings.....	829
<b>Chapter 76: Script Monitor</b> .....	<b>833</b>
Script Monitor Overview .....	833
Set a Timeout Value for Script Monitor Instances .....	839
Script Monitor Settings.....	840
<b>Chapter 77: Service Monitor</b> .....	<b>847</b>
Service Monitor Overview .....	848
Service Monitor Settings.....	850

<b>Chapter 78: Siebel Application Server Monitor</b> .....	<b>855</b>
Siebel Application Server Monitor Overview .....	856
Siebel Application Server Monitor Settings.....	861
<b>Chapter 79: Siebel Log File Monitor</b> .....	<b>867</b>
Siebel Log File Monitor Overview .....	868
Siebel Log File Monitor Settings.....	869
<b>Chapter 80: Siebel Web Server Monitor</b> .....	<b>873</b>
Siebel Web Server Monitor Overview .....	873
Siebel Web Server Monitor Settings .....	876
<b>Chapter 81: SNMP Monitor</b> .....	<b>881</b>
SNMP Monitor Overview .....	882
SNMP Monitor Settings .....	884
<b>Chapter 82: SNMP by MIB Monitor</b> .....	<b>891</b>
SNMP by MIB Monitor Overview.....	891
Configure the SNMP by MIB Monitoring Environment .....	893
SNMP by MIB Monitor Settings .....	895
<b>Chapter 83: SNMP Trap Monitor</b> .....	<b>901</b>
SNMP Trap Monitor Overview .....	901
SNMP Trap Monitor Settings.....	903
<b>Chapter 84: Solaris Zones Monitor</b> .....	<b>907</b>
Solaris Zones Monitor Overview .....	907
Analyze Solaris Zones Monitor Results - Use-Case Scenario .....	912
Solaris Zones Monitor Settings.....	914
<b>Chapter 85: SunONE Web Server Monitor</b> .....	<b>917</b>
SunONE Web Server Monitor Overview .....	917
SunONE Web Server Monitor Settings.....	919
<b>Chapter 86: Sybase Monitor</b> .....	<b>923</b>
Sybase Monitor Overview .....	923
Sybase Monitor Settings .....	925
<b>Chapter 87: Tuxedo Monitor</b> .....	<b>927</b>
Tuxedo Monitor Overview .....	927
Tuxedo Monitor Settings.....	930
<b>Chapter 88: UDDI Monitor</b> .....	<b>933</b>
UDDI Monitor Overview.....	933
UDDI Monitor Settings .....	934

<b>Chapter 89: UNIX Resources Monitor</b> .....	<b>935</b>
UNIX Resources Monitor Overview .....	935
UNIX Resources Monitor Settings.....	937
<b>Chapter 90: URL Monitor</b> .....	<b>941</b>
URL Monitor Overview .....	941
Configure the URL Monitoring Environment .....	946
URL Monitor Settings .....	948
<b>Chapter 91: URL Content Monitor</b> .....	<b>959</b>
URL Content Monitor Overview .....	959
Configure the URL Content Monitoring Environment.....	962
URL Content Monitor Settings .....	963
<b>Chapter 92: URL List Monitor</b> .....	<b>973</b>
URL List Monitor Overview .....	973
Configure the URL List Monitoring Environment .....	977
URL List Monitor Settings .....	978
<b>Chapter 93: URL Sequence Monitor</b> .....	<b>983</b>
URL Sequence Monitor Overview .....	983
Create a URL Sequence.....	997
URL Sequence Monitor User Interface.....	1000
<b>Chapter 94: VMware Performance Monitor</b> .....	<b>1015</b>
VMware Performance Monitor Overview .....	1015
Configure the VMware Performance Monitoring Environment ....	1019
Import the VMware Server Certificates .....	1020
VMware Performance Monitor Settings.....	1021
<b>Chapter 95: Web Script Monitor</b> .....	<b>1025</b>
Web Script Monitor Overview .....	1026
Configure the Web Script Monitoring Environment .....	1035
Web Script Monitor Settings .....	1037
<b>Chapter 96: Web Server Monitor</b> .....	<b>1043</b>
Web Server Monitor Overview .....	1043
Web Server Monitor Settings.....	1044
<b>Chapter 97: Web Service Monitor</b> .....	<b>1049</b>
Web Service Monitor Overview .....	1050
Web Service Monitor Settings .....	1055

<b>Chapter 98: WebLogic Application Server Monitor .....</b>	<b>1061</b>
WebLogic Application Server Monitor Overview .....	1062
Configure the WebLogic Application Server Monitoring Environment.....	1063
WebLogic Application Server Monitor Settings.....	1066
<b>Chapter 99: WebSphere Application Server Monitor .....</b>	<b>1071</b>
WebSphere Application Server Monitor Overview .....	1072
Configure the WebSphere 3.5x and 4.x Application Server Monitoring Environment .....	1074
Configure the WebSphere 5.x Application Server Monitoring Environment .....	1075
Configure the WebSphere 6.0x Application Server Monitoring Environment .....	1077
Configure the WebSphere 6.1x Application Server Monitoring Environment .....	1083
Configure the WebSphere 7.0x Application Server Monitoring Environment .....	1090
WebSphere Application Server Monitor Settings.....	1097
<b>Chapter 100: WebSphere MQ Status Monitor .....</b>	<b>1103</b>
WebSphere MQ Status Monitor Overview .....	1104
Configure the WebSphere MQ Status Monitoring Environment ..	1107
Channel Status Codes .....	1109
WebSphere MQ Status Monitor Settings.....	1110
<b>Chapter 101: WebSphere Performance Servlet Monitor .....</b>	<b>1113</b>
WebSphere Performance Servlet Monitor Overview .....	1113
WebSphere Performance Servlet Monitor Settings .....	1115
<b>Chapter 102: XML Metrics Monitor .....</b>	<b>1119</b>
XML Metrics Monitor Overview .....	1120
XML Metrics Monitor Settings.....	1122

**PART IV: INTEGRATION MONITORS**

<b>Chapter 103: Working with SiteScope Integration Monitors .....</b>	<b>1129</b>
Integration Monitors Overview .....	1130
Topology Settings for Technology Integration Monitors .....	1133
Deploy Integration Monitors .....	1140
List of Deprecated Integration Monitors.....	1142
Troubleshooting and Limitations .....	1143



<b>Chapter 104: Integration Monitor Field Mapping .....</b>	<b>1147</b>
Integration Monitor Field Mapping Overview.....	1148
Understanding Field Mapping Structure.....	1149
Configuring Field Mapping for Event Samples.....	1150
Configuring Field Mapping for Measurement Samples.....	1156
Configuring Field Mapping for Ticket Samples .....	1159
Event Handler Structure .....	1163
<b>Chapter 105: HP OM Event Monitor.....</b>	<b>1173</b>
HP OM Event Monitor Overview .....	1174
HP OM Integration Add-on – Workflow.....	1175
HP OM Event Monitor User Interface.....	1183
<b>Chapter 106: HP Service Manager Monitor .....</b>	<b>1187</b>
HP Service Manager Monitor Overview .....	1188
HP Service Manager Integration – Workflow.....	1189
HP Service Manager Monitor User Interface.....	1192
<b>Chapter 107: NetScout Event Monitor .....</b>	<b>1197</b>
NetScout Event Monitor Overview .....	1198
NetScout Integration – Workflow .....	1200
NetScout Event Monitor User Interface .....	1201
<b>Chapter 108: Technology Database Integration Monitor.....</b>	<b>1205</b>
Technology Database Integration Monitor Overview .....	1206
Integrate Database Data into HP Business Availability Center.....	1210
Technology Database Integration Monitor User Interface .....	1214
Troubleshooting and Limitations .....	1223
<b>Chapter 109: Technology Log File Integration Monitor .....</b>	<b>1225</b>
Technology Log File Integration Monitor Overview .....	1226
Integrate Log File Data into HP Business Availability Center.....	1228
Technology Log File Integration Monitor User Interface .....	1232
Troubleshooting and Limitations .....	1240
<b>Chapter 110: Technology SNMP Trap Integration Monitor .....</b>	<b>1241</b>
Technology SNMP Trap Integration Monitor Overview.....	1242
Integrate SNMP Trap Data into HP Business Availability Center ...	1243
Technology SNMP Trap Integration Monitor Settings .....	1247
Troubleshooting and Limitations .....	1253

<b>Chapter 111: Technology Web Service Integration Monitor</b> .....	<b>1257</b>
Technology Web Service Integration Monitor Overview .....	1258
Check Connectivity to the Technology Web Service Integration Monitor .....	1261
Technology Web Service Integration Monitor Settings.....	1262
Troubleshooting and Limitations .....	1267
<b>Chapter 112: Integration with HP Network Node Manager</b> .....	<b>1269</b>
Network Node Manager Integration Overview .....	1269
Writing Scripts to Export Network Node Manager Data .....	1270
Configure Events in Network Node Manager .....	1271

**PART V: REMOTE SERVERS**

<b>Chapter 113: Working with Remote Servers</b> .....	<b>1275</b>
Remote Servers Overview .....	1276
Configure SiteScope to Monitor a Remote Microsoft Windows Server .....	1277
Configure SiteScope to Monitor a Remote UNIX Server .....	1285
Remote Servers User Interface .....	1287
Troubleshooting and Limitations .....	1309
<b>Chapter 114: SiteScope Monitoring Using Secure Shell (SSH)</b> .....	<b>1317</b>
SiteScope and SSH Overview .....	1318
Monitoring Remote Windows Servers Using SSH.....	1322
Configure Remote UNIX Servers for SSH monitoring .....	1324
Configure Remote Windows Servers for SSH monitoring .....	1325
SSH Configuration Requirements For UNIX Remote Servers .....	1340
Monitors Supporting Perfex/Non-Perfex Based NT SSH .....	1341
Troubleshooting and Limitations .....	1343
<b>Chapter 115: Working with SSH Clients</b> .....	<b>1345</b>
Integrated Java SSH Client Overview .....	1346
External SSH Client Overview .....	1348
Configure the Integrated Java SSH Client.....	1351
Configure the External SSH Client.....	1355
<b>Chapter 116: UNIX Operating System Adapters</b> .....	<b>1363</b>
SiteScope UNIX Operating System Adapters Overview .....	1363
Add an Adapter.....	1364
UNIX Adapters Provided with SiteScope.....	1365
Adapter File Format .....	1366
Adapter Command List .....	1367

**PART VI: PREFERENCES**

<b>Chapter 117: General Preferences .....</b>	<b>1375</b>
General Preferences Overview .....	1376
General Preferences User Interface .....	1379
<b>Chapter 118: Infrastructure Preferences .....</b>	<b>1387</b>
Infrastructure Preferences Overview .....	1387
Infrastructure Preferences User Interface .....	1388
<b>Chapter 119: Integration Preferences .....</b>	<b>1415</b>
Integration Preferences Overview .....	1416
Configure SiteScope-HP Business Availability Center	
Integration Preferences for Inaccessible Profiles .....	1423
XML Tag Reference for Generic Data Integration .....	1426
Integration Preferences User Interface .....	1429
<b>Chapter 120: Log Preferences .....</b>	<b>1449</b>
Log Preferences Overview .....	1449
SiteScope Log Database Table Structure .....	1450
Log Preferences User Interface .....	1452
Troubleshooting and Limitations .....	1455
<b>Chapter 121: Failover Preferences .....</b>	<b>1457</b>
Failover Preferences Overview .....	1457
Failover Preferences User Interface .....	1458
<b>Chapter 122: Email Preferences .....</b>	<b>1461</b>
Email Preferences Overview .....	1461
Email Preferences User Interface .....	1462
<b>Chapter 123: Pager Preferences .....</b>	<b>1471</b>
Pager Preferences Overview .....	1472
Pager Preferences User Interface .....	1473
<b>Chapter 124: SNMP Trap Preferences .....</b>	<b>1481</b>
SNMP Trap Preferences Overview .....	1481
SNMP Trap Preferences User Interface .....	1482
<b>Chapter 125: Schedule Preferences .....</b>	<b>1487</b>
Schedule Preferences Overview .....	1487
Schedule Preferences User Interface .....	1490
<b>Chapter 126: User Management Preferences .....</b>	<b>1497</b>
User Management Preferences Overview .....	1498
Password Requirement Parameters .....	1503
User Management Preferences User Interface .....	1504

<b>Chapter 127: Credential Preferences</b> .....	<b>1523</b>
Credential Preferences Overview .....	1524
Configure Credential Preferences .....	1527
Credential Preferences User Interface .....	1528
<b>Chapter 128: Search/Filter Tags</b> .....	<b>1533</b>
Search/Filter Tags Overview .....	1533
Search/Filter Tags User Interface .....	1534
<b>Chapter 129: Certificate Management</b> .....	<b>1535</b>
Certificate Management Overview .....	1536
Import Server Certificates Using Certificate Management .....	1537
Certificate Management User Interface .....	1538
<b>Chapter 130: Using SiteScope in an Internationalization (I18N)</b>	
<b>Environment</b> .....	<b>1545</b>
Multi-Lingual User (MLU) Interface Support.....	1546
Configure SiteScope for a Non-English Locale .....	1547
View SiteScope User Interface in a Specific Language .....	1549
Monitors Tested for Internationalization .....	1550
Troubleshooting and Limitations .....	1552

**PART VII: TEMPLATES**

<b>Chapter 131: SiteScope Templates</b> .....	<b>1557</b>
SiteScope Templates Overview .....	1558
Understanding Templates .....	1561
Template Examples .....	1564
Planning Templates.....	1565
Working with Template Variables .....	1567
Counter Selection in Monitor Templates .....	1573
Deploying a Template Using a CSV File .....	1577
Updating Template Deployments .....	1578
Configure a SiteScope Monitoring Solution Using a Template – Workflow.....	1580
Publish Template Updates to Related Group Deployments .....	1596
Modify Counter Selection Strings to Use Regular Expressions.....	1601
Export and Import a Template.....	1602
Reserved Template Group Types.....	1603
SiteScope Templates User Interface.....	1604

<b>Chapter 132: Auto Template Deployment .....</b>	<b>1643</b>
Auto Template Deployment Overview .....	1644
Creating and Working with the XML File .....	1645
XML File Example and Variables .....	1646
XML Validator .....	1650
Publishing Template Changes Using the XML .....	1650
Deployment Results.....	1653
Deploy a Monitoring Structure Using an XML File .....	1653
Encrypt Text .....	1657
Update a Deployment .....	1658
XML Tag Reference.....	1660
Troubleshooting and Limitations .....	1663
<b>Chapter 133: SiteScope Solution Templates .....</b>	<b>1665</b>
Solution Templates Overview .....	1665
Deploy a SiteScope Solution Template – Workflow.....	1669
Solution Template User Interface.....	1671
Troubleshooting and Limitations .....	1672
<b>Chapter 134: Active Directory Solution Template.....</b>	<b>1673</b>
Active Directory Solution Overview.....	1673
Deploy the Active Directory Solution Template .....	1675
Active Directory Solution Template User Interface .....	1676
<b>Chapter 135: AIX Host Solution Templates .....</b>	<b>1679</b>
AIX Host Solution Overview .....	1679
Deploy the AIX Host Solution Template .....	1681
AIX Host Solution Configuration Requirements .....	1682
AIX Host Solution Template User Interface.....	1682
<b>Chapter 136: HP Quality Center Solution Templates.....</b>	<b>1685</b>
HP Quality Center Solution Templates Overview.....	1686
Deploy the HP Quality Center Solution Template .....	1689
HP Quality Center Solution Template Configuration Requirements .....	1690
HP Quality Center Solution Template User Interface.....	1692
Troubleshooting and Limitations .....	1702
<b>Chapter 137: HP Service Manager Solution Template.....</b>	<b>1703</b>
HP Service Manager Solution Overview.....	1704
Deploy the HP Service Manager Solution Template .....	1705
HP Service Manager Solution Configuration Requirements.....	1706
HP Service Manager Solution Template User Interface.....	1707

<b>Chapter 138: JBoss Application Server Solution Template .....</b>	<b>1711</b>
JBoss Application Server Solution Overview .....	1712
Deploy the JBoss Application Server Solution Template .....	1713
JBoss Solution Configuration Requirements.....	1714
JBoss Solution Template User Interface .....	1715
<b>Chapter 139: Linux Host Solution Templates .....</b>	<b>1719</b>
Linux Host Solution Overview .....	1719
Deploy the Linux Host Solution Template .....	1721
Linux Host Solution Configuration Requirements.....	1722
Linux Host Solution Template User Interface.....	1722
<b>Chapter 140: Microsoft Exchange Solution Templates .....</b>	<b>1725</b>
Microsoft Exchange Solution Overview.....	1726
Deploy Microsoft Exchange Solution Templates.....	1728
Microsoft Exchange Solution Configuration Requirements.....	1729
Microsoft Exchange Solution Template User Interface .....	1729
<b>Chapter 141: Microsoft IIS Solution Template .....</b>	<b>1733</b>
Microsoft IIS Solution Overview .....	1734
Deploy the Microsoft IIS Solution Template .....	1735
Microsoft IIS Solution Configuration Requirements .....	1736
Microsoft IIS Solution Template User Interface .....	1736
<b>Chapter 142: Microsoft SQL Server 2005 Solution Template .....</b>	<b>1739</b>
Microsoft SQL Server 2005 Solution Overview .....	1739
Deploy the Microsoft SQL Server 2005 Solution Template .....	1741
Microsoft SQL Server 2005 Solution Configuration Requirements .....	1742
Microsoft SQL Server 2005 Solution Template User Interface.....	1743
<b>Chapter 143: Microsoft Windows Host Solution Template .....</b>	<b>1747</b>
Microsoft Windows Host Solution Overview .....	1747
Deploy the Microsoft Windows Host Solution Template.....	1749
Microsoft Windows Host Solution Configuration Requirements .....	1750
Microsoft Windows Host Solution Template User Interface .....	1751
<b>Chapter 144: .NET Solution Templates.....</b>	<b>1753</b>
.NET Solution Overview .....	1753
Deploy the .NET Solution Template .....	1755
.NET Solution Configuration Requirements.....	1756
.NET Solution Template User Interface.....	1756

<b>Chapter 145: Oracle Database Solution Template .....</b>	<b>1759</b>
Oracle Database Solution Overview .....	1760
Deploy Oracle Database Solution Templates .....	1762
Oracle Database Solution Template Usage Guidelines .....	1763
Oracle Database Solution Template Tools .....	1763
Oracle Solution Template User Interface .....	1766
<b>Chapter 146: SAP Solution Templates .....</b>	<b>1769</b>
SAP Solution Overview .....	1770
Deploy the SAP Solution Template .....	1771
SAP Solution Template Configuration Requirements.....	1772
SAP Solution Template User Interface.....	1773
<b>Chapter 147: Siebel Solution Templates.....</b>	<b>1777</b>
Siebel Solution Overview.....	1778
Deploy the Siebel Solution Template.....	1780
Siebel Solution Configuration Requirements .....	1781
Siebel Solution Template User Interface .....	1782
<b>Chapter 148: Solaris Host Solution Templates .....</b>	<b>1789</b>
Solaris Host Solution Overview .....	1789
Deploy the Solaris Host Solution Template .....	1791
Solaris Host Solution Configuration Requirements.....	1792
Solaris Host Solution Template User Interface.....	1792
<b>Chapter 149: WebLogic Solution Template.....</b>	<b>1795</b>
WebLogic Solution Overview.....	1796
Deploy the WebLogic Solution Template .....	1798
WebLogic Solution Usage Guidelines .....	1799
Selecting WebLogic Modules for Monitoring .....	1799
WebLogic Solution Template User Interface.....	1801
<b>Chapter 150: WebSphere Solution Template.....</b>	<b>1805</b>
WebSphere Solution Overview.....	1805
Deploy the WebSphere Solution Template.....	1807
WebSphere Solution Template User Interface .....	1808

<b>Chapter 151: Monitor Deployment Wizard</b> .....	<b>1811</b>
Monitor Deployment Wizard Overview .....	1812
Prerequisites for Running the Monitor Deployment Wizard .....	1814
Monitor Deployment Wizard Templates and Variables .....	1816
Full and Partial Monitor Coverage .....	1818
Wizard Options .....	1819
Monitor Deployment Wizard for Siebel.....	1820
Deploy Monitors Using the Monitor Deployment Wizard .....	1821
Template Reference .....	1827
Monitor Deployment Wizard User Interface .....	1835

**PART VIII: SITESCOPE DASHBOARD**

<b>Chapter 152: Working with SiteScope Dashboard</b> .....	<b>1847</b>
SiteScope Dashboard Overview .....	1848
Dashboard Filter Overview.....	1849
Acknowledging Monitor Status.....	1850
Accessing SiteScope Tools .....	1851
Customize SiteScope Dashboard .....	1851
Analyze Data in SiteScope Dashboard .....	1853
SiteScope Dashboard User Interface.....	1856
<b>Chapter 153: Server-Centric Report</b> .....	<b>1881</b>
Generating a Server-Centric Report .....	1881
Create a Server-Centric Report – Workflow .....	1883
Create a Server-Centric Report – Scenario.....	1885
Server-Centric Report Measurements.....	1889
Server-Centric Report .....	1890
<b>Chapter 154: SiteScope Server Health</b> .....	<b>1895</b>
SiteScope Health Overview.....	1896
SiteScope Health Group .....	1899
BAC Integration Configuration Monitor .....	1900
BAC Integration Statistics Monitor .....	1901
SiteScope Log Events Monitor.....	1901
SiteScope Monitor Load Monitor .....	1902
SiteScope Server Health Monitor.....	1902
Analyze SiteScope Health Monitor Data .....	1903
SiteScope Health User Interface .....	1906



<b>Chapter 155: Viewing Server Statistics</b> .....	<b>1921</b>
Using Server Statistics.....	1922
Interpreting SiteScope Server Load Statistics .....	1923
Using Log Files.....	1927
Analyze SiteScope Server Statistics .....	1930
Configure the Audit Log.....	1931
SiteScope Log File Columns .....	1932
Audit Log Entries .....	1933
SiteScope Server Statistics User Interface.....	1943

## **PART IX: ALERTS AND REPORTS**

<b>Chapter 156: SiteScope Alerts</b> .....	<b>1959</b>
SiteScope Alerts Overview .....	1960
Creating Alert Actions .....	1963
Understanding When SiteScope Alerts Are Sent .....	1964
Customizing Alert Templates .....	1969
Working with Database Alerts.....	1971
Working with Disable or Enable Monitor Alerts .....	1972
Working with Email Alerts .....	1973
Working with Log Event Alerts .....	1974
Working with Pager Alerts .....	1975
Working with Post Alerts .....	1976
Working with Script Alerts .....	1977
Working with SMS Alerts .....	1981
Working with SNMP Trap Alerts .....	1982
Working with Sound Alerts.....	1983
Configure an Alert .....	1984
Customize an Alert's Message Content.....	1986
Customize Alert Template Tag Styles .....	1988
SiteScope Alert Templates Directory .....	1989
SiteScope Alert Template Properties Directory.....	1990
SiteScope Alerts User Interface .....	1997
<b>Chapter 157: Writing Scripts for Script Alerts</b> .....	<b>2029</b>
Writing Scripts for Script Alerts Overview .....	2029
Working with Scripts in SiteScope .....	2030
Passing Data from SiteScope to a Script .....	2032

- Chapter 158: SiteScope Reports .....2035**
- SiteScope Reports Overview .....2035
- SiteScope Report Types .....2037
- Working with SiteScope Management Reports.....2039
- Create a Report .....2041
- SiteScope Reports User Interface .....2042
  
- Chapter 159: System Availability Management Reports.....2091**
- System Availability Management Reports Overview .....2092
- Working with System Availability Management Reports.....2093
- SiteScope Over Time Reports.....2095
- Understanding the Cross-Performance Report Scale .....2098
- Understanding the Group Performance Report.....2099
- System Availability Management Data in Custom Reports.....2100
- Create a Monitor Performance Report – Workflow .....2102
- Create a Cross-Performance Report – Workflow.....2103
- Rescale a Cross-Performance Report .....2104
- System Availability Management Reports User Interface .....2104
  
- Chapter 160: Event Log.....2137**
- Event Log Overview .....2138
- View the Event Log - Workflow .....2139
- Customize the Event Log .....2141
- Set Additional Filters for SiteScope .....2142
- Event Log User Interface .....2142
  
- Index .....2151**

---

# Welcome to This Guide

This guide describes how to use the System Availability Management application to monitor the enterprise IT infrastructure.

**This chapter includes:**

- ▶ How This Guide Is Organized on page 27
- ▶ Who Should Read This Guide on page 29
- ▶ Getting More Information on page 29

## How This Guide Is Organized

The guide contains the following parts:

**Part I Introduction to SiteScope**

Introduces SiteScope and provides an overview of the SiteScope key features, architecture, monitoring model, and a working order for using SiteScope to monitor your organization's IT infrastructure. In addition, it describes how to access SiteScope and use a silent login.

**Part II General and Administration**

It describes how to navigate the SiteScope user interface, search and filter SiteScope objects, use Global Search and Replace, use SiteScope tools to troubleshoot resource and monitor configuration problems, and use regular expressions. It also describes how to use System Availability Management Administration from within HP Business Availability Center to register, configure, and maintain multiple SiteScopes.

### **Part III Monitors**

Describes how to configure each type of SiteScope monitor. It also describes how to monitor XML documents.

### **Part IV Integration Monitors**

Describes how to configure each type of integration monitor, including troubleshooting issues relating to monitoring EMS environments with SiteScope.

### **Part V Remote Servers**

Describes how to set up connection properties so that SiteScope can monitor in remote environments. It also describes how to use Secure Shell (SSH) connection for remote server monitoring, configure clients working with SSH, and create and customize adapter files for UNIX monitoring.

### **Part VI Preferences**

It describes how to configure the SiteScope's general and administrative functions, including infrastructure, integration, logs, settings for connecting to email, pager and SNMP systems, schedule profiles, user profiles, and credential management.

### **Part VII Templates**

Describes how to use templates to efficiently deploy, maintain, and update monitoring solutions, including groups, monitors, remote servers, and alerts. It also describes deploying SiteScope monitoring for commonly used IT applications using solution templates. It also describes using the Monitor Deployment Wizard.

### **Part VIII SiteScope Dashboard**

Describes how to use the SiteScope Dashboard tab to view the latest real-time monitor data and to customize the display of monitor results. It also describes monitoring SiteScope server health, and viewing server statistics and logs.

## Part IX Alerts and Reports

Describes how to use SiteScope Alerts to send notifications of an event or change of status in your infrastructure, and how to customize alert templates and write script alerts. It also describes how to create SiteScope Reports to define the monitor parameters, time interval, or summary data you want to measure. It also describes using System Availability Management reports.

## Who Should Read This Guide

This guide is intended for the following users of HP Business Availability Center:

- SiteScope administrators
- SiteScope application administrators
- SiteScope data collector administrators
- SiteScope end users

Readers of this guide should be knowledgeable about enterprise system administration, infrastructure monitoring systems, and SiteScope, and have familiarity with the systems being set up for monitoring. In addition, readers who are integrating with HP Business Availability Center should be familiar with HP Business Availability Center and enterprise monitoring and management concepts.

## Getting More Information

For a complete list of all online documentation included with HP SiteScope, additional online resources, information on acquiring documentation updates, and typographical conventions used in this guide, see the *HP SiteScope Deployment Guide* PDF.

Welcome to This Guide

# Part I

---

## Introduction to SiteScope





# 1

---

## Introducing SiteScope

This chapter introduces the SiteScope monitoring model.

### **This chapter includes:**

#### **Concepts**

- SiteScope Overview on page 34
- Key Features of SiteScope on page 35
- SiteScope Architecture on page 36
- SiteScope Monitoring Model on page 37
- Using a Silent Login on page 38
- Using the JMX Console on page 39

#### **Tasks**

- Access SiteScope on page 40
- Create a Silent Login URL on page 42
- Setup and Administration on page 45
- Configure SiteScope for Monitoring – Workflow on page 48
- Configure a SiteScope Monitoring Solution Using a Template – Flowchart on page 51

## **SiteScope Overview**

HP SiteScope is an agentless monitoring solution designed to ensure the availability and performance of distributed IT infrastructures—for example, servers, operating systems, network devices, network services, applications, and application components. This Web-based infrastructure monitoring solution is lightweight, highly customizable, and does not require that data collection agents be installed on your production systems.

SiteScope has over 90 types of monitors that can monitor utilization, response time, usage, and resource availability of a variety of host types and application platforms. SiteScope can be configured to alert whenever it detects a problem in the IT infrastructure. There are several types of alert actions, such as sending email messages, paging, sending Simple Network Management Protocol (SNMP) traps, or executing a script.

You can create a report for a single monitor, several monitors, or even several monitor groups. SiteScope reports display information about how the servers and applications you are monitoring have performed over time. SiteScope reports are important tools in monitoring and troubleshooting operational performance and availability and reviewing the monitored environment.

SiteScope provides different tools, such as templates, the Publish Template Changes wizard, and automatic template deployment that enable you to develop a standardized set of monitor types and configurations into a single structure. SiteScope templates can be speedily deployed across the enterprise and quickly updated to make sure that the monitoring infrastructure is compliant with the standards set in the template. SiteScope also includes alert types that you can use to communicate and record event information in a variety of media. You can customize alert templates to meet the needs of your organization.

SiteScope monitors key aspects of its own operability and identifies monitor configuration problems and critical server load. It also monitors its own integration and data events when configured to report to HP Business Availability Center.

## Key Features of SiteScope

SiteScope has the following features:

- ▶ **Agentless monitoring.** SiteScope monitors without the deployment of agent software on the servers to be monitored. This function makes deployment and maintenance of SiteScope relatively simple compared to other performance monitoring solutions.
- ▶ **Enterprise-ready architecture.** SiteScope provides failover capabilities, simultaneous monitoring of large number of systems, and support for secure connections.
- ▶ **Simple installation and deployment.** SiteScope is installed on a single server running as a service or a process. This results in quick installation and easy monitoring configuration.
- ▶ **Infrastructure performance and availability monitoring.** SiteScope has over 90 types of monitors. SiteScope can monitor utilization, response time, usage, and resource availability of a variety of host types and application platforms.
- ▶ **Standardized monitor deployments and updates using templates.** SiteScope templates, the Publish Template Changes wizard, and automatic template deployment provide an enterprise solution for standardizing the monitoring of the different IT elements in your enterprise. Templates speed the deployment of monitors across the enterprise through the single-operation deployment of groups, monitors, alerts, remote servers, and configuration settings in a single structure that can be repeatedly deployed and updated.
- ▶ **Proactive alerting.** SiteScope can be configured to alert whenever it detects a problem in the IT infrastructure. There are several types of alert actions, such as sending email messages, paging, sending Simple Network Management Protocol (SNMP) traps, or executing a script.
- ▶ **Self-monitoring.** SiteScope monitors key aspects of its own operability and identifies monitor configuration problems and critical server load. It also monitors its own integration and data events when configured to report to HP Business Availability Center.

- ▶ **Customization capabilities.** SiteScope allows for display of customizations of groups and monitors by using custom data fields and HTML-sensitive description tags. In addition, SiteScope allows for the customization of alert text and report configurations by using templates and user-defined variables.
- ▶ **Intuitive administration.** SiteScope reduces the time spent managing a monitoring environment by providing a user friendly browser-based interface for viewing and administering of the monitoring platform.

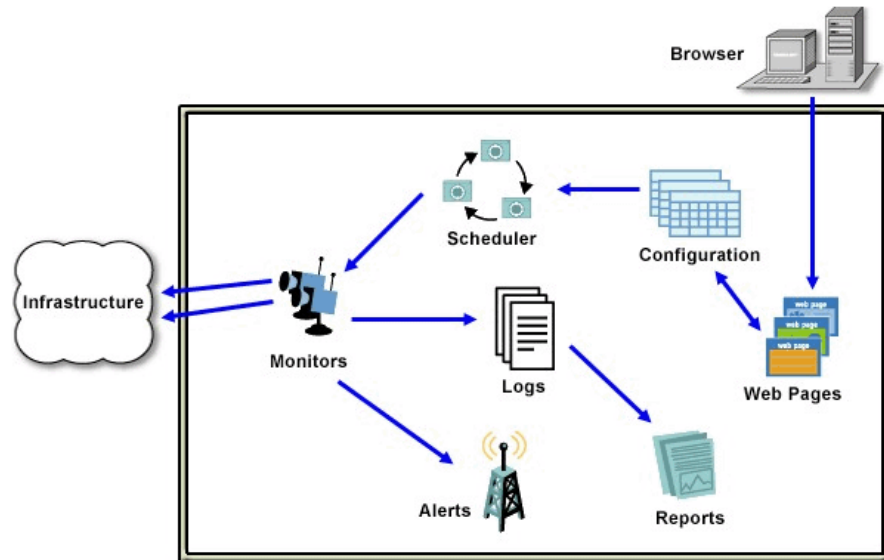
## SiteScope Architecture

SiteScope's Web-enabled architecture allows for the creation and ongoing administration of a scalable monitoring environment. It consists of the following components:

- ▶ **Browser-based interface.** Manages end user status information requests, configuration change requests, and access control.
- ▶ **Scheduler.** Coordinates the running of monitors, alert creation, and report generation.
- ▶ **Monitors.** Collect performance and availability information about the system being monitored.
- ▶ **Alerts.** Notifications of exceptions, failures, and status change events in the system being monitored.
- ▶ **Reports.** A historical representation of monitored data for trending and analysis purposes.

## SiteScope Monitoring Model

The SiteScope monitoring model is displayed in the diagram below.



SiteScope architecture is comprised of the following key components:

- ▶ **Groups.** A group is a container for monitoring assets. Groups may contain subgroups and are used to organize monitors. Groups are created prior to monitors.
- ▶ **Monitors.** A monitor checks the status of server components, key application processes, log files, or network devices, to name a few. It collects data based on selected metrics and displays a status of good, warning, or error with respect to the configured thresholds.
- ▶ **Alerts.** An alert is an action triggered by a change in the status of a monitored asset. Alerts notify required users when negative events or failures occur. An alert can be sent to a variety of media including email, pager, Short Message Service (SMS) messages, or an SNMP trap.
- ▶ **Reports.** A report is a historical representation of monitored data. SiteScope offers a variety of reports from quick monitor reports to detailed management reports. Reports enable you to track trends and operational performance and to troubleshoot problems.

## Using a Silent Login

Silent login is an automatic process that launches SiteScope without having to enter the user login name and password in the SiteScope login page. This enables you to skip the initial login page and instead go directly to a SiteScope client. In addition, you can use silent login in conjunction with a page option view that you saved in your browser's list of Favorites to open SiteScope directly to a particular group or view. For details on configuring a favorite page option view, see Page Options in "SiteScope Common Toolbar" on page 58.

To start SiteScope using silent login, you must encrypt the user login name and password using the SiteScope Encryption Tool, and enter the encrypted information in the silent login URL. The URL is in the format:

```
http://<server_name>:8080/SiteScope?sis_silent_login_type=encrypted&login=
<encrypted_login_name>&password=<encrypted_password>
```

For details on how to create a SiteScope silent login URL, see "Create a Silent Login URL" on page 42.

## Using the JMX Console

SiteScope includes the Java monitoring and management instrumentation (JConsole) tool. This tool uses Java Management Extension (JMX) technology to provide information on performance and resource consumption of applications running on the Java platform.

You can use JConsole to perform remote management operations, view performance of processes, and troubleshoot problematic areas of SiteScope. This tool may help in debugging difficult issues related to memory consumption, threading, and other issues in the production environment.

You can access the JConsole tool by running  
<SiteScope root directory>\java\bin\jconsole.exe on Windows platforms (and <SiteScope root directory>/java/bin/jconsole binary file on UNIX platforms). Depending on which SiteScope you want to monitor, select **Local**, or **Remote** with port **27676**.

Since access to the JMX server is not password protected (JConsole password authentication is disabled by default in SiteScope), we recommend that you enable JMX password authentication to prevent unauthorized entry. For details, see “Enable JMX Server Password Protection - Optional” on page 47.

---

**Note:** We do not recommend changing any other JConsole settings.

---

## Access SiteScope

This task describes the various ways in which you can access SiteScope.

This task includes the following steps:

- “Access SiteScope from a Browser - Optional” on page 40
- “Access SiteScope from the Start Menu - Optional” on page 40
- “Access SiteScope Using Remote Login - Optional” on page 40
- “Results” on page 41

### **1 Access SiteScope from a Browser - Optional**

To access SiteScope, enter the SiteScope address in a Web browser. The default address is: <http://localhost:8080/SiteScope>.

### **2 Access SiteScope from the Start Menu - Optional**

On Windows platforms, you can also access SiteScope from the Start menu by clicking **Start > Programs > HP SiteScope > Open HP SiteScope**.

### **3 Access SiteScope Using Remote Login - Optional**

You can access SiteScope using a silent login. This enables you to skip the login page and directly open the user account for the given user name and password using the silent login address.

For details on this topic, see “Using a Silent Login” on page 38.

For details on how to perform this task, see “Create a Silent Login URL” on page 42.



## 4 Results

The first time SiteScope is deployed, there is a delay for initialization of the interface elements. When you connect to a SiteScope, the SiteScope opens to the Dashboard view.

---

**Note:** To restrict access to this account and its privileges, you need to edit the Administrator account profile to include a user login name and login password. SiteScope then displays a login dialogue before SiteScope can be accessed. If no user name and password are defined for the Administrator user, SiteScope skips the login page and automatically logs in. For details on editing the Administrator account profile, see “User Management Preferences Overview” on page 1498.

---

## Create a Silent Login URL

This task describes how to create a silent login URL which enables you to log on to the specified SiteScope server directly without showing the SiteScope login page.

This task includes the following steps:

- “Create a User Profile” on page 42
- “Configure User Permissions - Optional” on page 43
- “Encrypt the User Profile” on page 43
- “Create a SiteScope Silent Login URL for the User Profile” on page 44
- “Results” on page 44

### 1 Create a User Profile

In the **Preferences** context, click the **User Management Preferences** menu and create a user account.

For details on the user interface, see “User Management Preferences User Interface” on page 1504.

---

**Note:** The Administrator account is the default account that is active when the product is installed. To create other accounts, you must first edit the Administrator account profile to include a user login name and login password.

---

**Example**

A user profile with the displayed name Regular User was added with login name Regular and password Regular.

The screenshot shows a 'New User' dialog box with the following fields and values:

- Displayed user name: Regular User
- Login name: Regular
- Password: \*\*\*\*\*
- Confirm password: \*\*\*\*\*
- LDAP service provider: (empty)
- LDAP security principal: (empty)
- Login disabled
- Allowed groups: SiteScope

The dialog also features a 'Permissions' section at the bottom and 'OK', 'Cancel', and 'Help' buttons.

**2 Configure User Permissions - Optional**

Configure the user action permissions in the **Permissions** section of the New/Edit User dialog box. By default, a new user has full permissions except for the permission to modify or delete other user preferences.

For details on the user interface, see “New/Edit User Profile Dialog Box” on page 1505.

**3 Encrypt the User Profile**

Encrypt the user login name and password.

- a** In a command prompt, run the following command for the login name:  
`<SiteScope root directory>\tools\AutoDeployment\encrypt_password.bat <login name>`

For example:

```
C:\SiteScope\tools\AutoDeployment\encrypt_password.bat Regular
```

The encrypted value for Regular is (sisp)uq1zrGI1lms=.

- b** Encode any non-standard URL characters according to the list in <http://www.blooberry.com/indexdot/html/topics/urlencoding.htm>. Note that URL encoding of a character consists of a % symbol, followed by the two-digit representation for the character.

In this example, = is a reserved character, and should be replaced by %3D. Thus, the encoded value for Regular is (sisp)uq1zrG1lms%3D.

- c** Save the encrypted value so that you can add it to the silent login URL.
- d** Repeat the encryption process for the login password (if different from the login name).

#### **4 Create a SiteScope Silent Login URL for the User Profile**

Enter the SiteScope silent login URL in a Web browser. The URL should be in the format:

```
http://<server_name>:8080/SiteScope?sis_silent_login_type=encrypted&login=
<encrypted_login_name>&password=<encrypted_password>
```

where <encrypted\_login\_name> and <encrypted\_password> are replaced by the encrypted login name and password.

#### **5 Results**

SiteScope skips the login page and directly opens the user account for the given user name and password.

---

**Note:** If values entered for the login name and password parameters either do not exist, are not found, or if authentication fails, then the SiteScope login page is displayed.

---

## Setup and Administration

This task describes a suggested working order for preparing to use SiteScope.

This task includes the following steps:

- “Log in to SiteScope” on page 45
- “Enter your SiteScope License” on page 45
- “Configure SiteScope Preferences” on page 45
- “Configure Connection Profiles for Remote Servers” on page 47
- “Install Middleware Drivers” on page 47
- “Enable JMX Server Password Protection - Optional” on page 47
- “Results” on page 48

### 1 Log in to SiteScope

Enter the SiteScope address in a Web browser. The default address is:  
<http://localhost:8080/SiteScope>.

### 2 Enter your SiteScope License

If you did not enter your SiteScope license information during installation, enter it in **Preferences > General Preferences > Main Panel**.

For details on the user interface, see “License number” on page 1379.

### 3 Configure SiteScope Preferences

Configure specific properties and settings related to administrative tasks within SiteScope.

- a Create a SiteScope user account.** The Administrator account is the default account that is active when the product is installed. It has full privileges to manage SiteScope and is the account that all users who access the product use unless you restrict the account. Create and configure other user accounts based on the requirements of the organization. For details on this topic, see “User Management Preferences Overview” on page 1498.

---

**Note:** If no user name and password are defined for the administrator user, SiteScope skips the login page and automatically logs in.

---

- b Configure the SiteScope restart schedule.** Restarting the SiteScope server is necessary for clearing problems and resetting monitors. For details on configuring this setting, see “SiteScope restart schedule” on page 1380.
- c Configure the SiteScope Email Preferences server.** Configure an administrators email address and specify a mail server that SiteScope can use to forward email messages and alerts to users. For details on the Email Preferences user interface, see “Email Preferences User Interface” on page 1462.
- d Adjust Log Preferences.** Set the number of days of monitor data that are retained on the SiteScope server. By default, SiteScope deletes logs older than 40 days. If you plan to have monitor data exported to an external database, prepare the database, the necessary drivers, and configure the Log Preferences as applicable. For details on the Log Preferences user interface, see “Log Preferences User Interface” on page 1452.
- e Configure SiteScope to report to HP Business Availability Center.** This enables logging of SiteScope monitor data to Business Availability Center. For details on this topic, see “Configuring the Integration” on page 152.
- f Configure credentials for SiteScope objects.** Use Credential Preferences to store and manage credentials for SiteScope objects that require user authentication. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.

---

**Note:** In addition, you can configure any of the other SiteScope preferences as required. For details, see “Preferences Menu” on page 93.

---

## 4 Configure Connection Profiles for Remote Servers

Specify the connection method for the remote servers you want to monitor in accordance with your security requirements.

For details on enabling SiteScope to monitor data on remote Windows servers, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.

For details on enabling SiteScope to monitor data on remote UNIX servers, see “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285.

## 5 Install Middleware Drivers

Install middleware drivers for connectivity with remote databases and applications for those monitors that require drivers.

For details, see the help for the specific monitor.

## 6 Enable JMX Server Password Protection - Optional

To prevent unauthorized entry to the JMX server embedded in SiteScope, enable password protection by setting the following system property when you start the JVM:

```
-Dcom.sun.management.jmxremote.authenticate=true
```

- On Windows platforms, you should also add or replace this argument in the Windows registry setting **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SiteScope\serviceParam**.

By default, the `-Dcom.sun.management.jmxremote.authenticate` parameter is set to `false` in `serviceParam`.

- On UNIX platforms, you should add this argument to the `<SiteScope root directory>/bin/start-monitor` script.

For details on how to configure the JVM, see the Java Sun documentation (<http://java.sun.com/j2se/1.5.0/docs/guide/management/agent.html#auth>).

For details on the JMX Console, see “Using the JMX Console” on page 39.

## 7 Results

You are now ready to use SiteScope.

- For a workflow on creating a basic monitoring structure in SiteScope, see “Configure SiteScope for Monitoring – Workflow” on page 48.
- For a workflow on how to create and develop templates to help speed the deployment of monitoring using standardized group structure, naming conventions, and configuration settings, see “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580.

## Configure SiteScope for Monitoring – Workflow

This task describes the working order for creating a basic monitoring structure in SiteScope.

---

**Note:** It is more efficient to use SiteScope templates, the Publish Template Changes wizard, and automatic template deployment than the basic monitoring method for standardizing the monitoring of the different IT elements in your enterprise. For a flowchart that shows the steps involved in configuring a monitoring solution using a template, see “Configure a SiteScope Monitoring Solution Using a Template – Flowchart” on page 51. For details on the workflow, see “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580.

---

This task includes the following steps:

- “Prerequisites” on page 49
- “Create Groups and Subgroups” on page 49
- “Create Monitor Instances” on page 49
- “Set Monitor Dependencies - Optional” on page 49
- “Set Monitor Thresholds - Optional” on page 50
- “Set Up Monitor and Group Alerts - Optional” on page 50



- “Set Up Monitor and Group Reports - Optional” on page 50
- “Results” on page 50

## **1 Prerequisites**

Check that the post-installation administration tasks have been performed before configuring SiteScope for monitoring.

For details on how to perform this task, see “Setup and Administration” on page 45.

## **2 Create Groups and Subgroups**

Create groups and subgroups to make deployment of monitors and associated alerts manageable and effective for your environment and organization. For example, you can create groups of locations, server types, network resources, and so forth.

For details on how to perform this task, see “Manage a Group – Workflow” on page 294.

## **3 Create Monitor Instances**

Select the monitor instances you want to add to the group.

For details on how to perform this task, see “Deploy a Monitor – Workflow” on page 323.

## **4 Set Monitor Dependencies - Optional**

Build dependencies between groups and key monitors to help control redundant alerting.

For details on this topic, see “Monitoring Group Dependencies” on page 307.

## **5 Set Monitor Thresholds - Optional**

Set thresholds for one or multiple monitors using a baseline, or manually set logic conditions that determine the reported status of each monitor instance.

- ▶ For details on how to set monitor thresholds using a baseline, see “Set Monitor Thresholds Using a Baseline” on page 327.
- ▶ For details on the user interface for setting monitor thresholds manually, see “Threshold Settings” on page 362.

## **6 Set Up Monitor and Group Alerts - Optional**

Create alerts to send notification of an event or change of status in some element or system in your infrastructure.

For details on how to configure alerts, see “Configure an Alert” on page 1984.

## **7 Set Up Monitor and Group Reports - Optional**

Create reports to display information about how the servers and applications you are monitoring have performed over time.

For details on how to create reports, see “Create a Report” on page 2041.

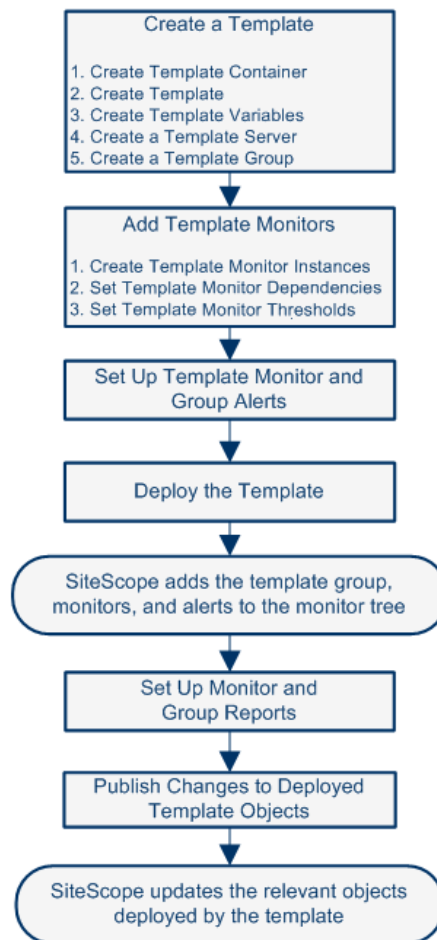
## **8 Results**

SiteScope adds the monitors, alerts, and reports to the specified container in the monitor tree.

## Configure a SiteScope Monitoring Solution Using a Template – Flowchart

The flowchart below shows the steps required to configure a SiteScope monitoring solution using SiteScope templates and the Publish Template Changes wizard. Templates are used to standardize a set of group structures, monitor types and configuration settings into a single structure that can be repeatedly deployed and updated.

For details on the workflow, see “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580.





# **Part II**

---

## **General and Administration**



# 2

---

## Navigating the SiteScope User Interface

This chapter introduces and explains how to navigate the SiteScope user interface.

### **This chapter includes:**

#### **Concepts**

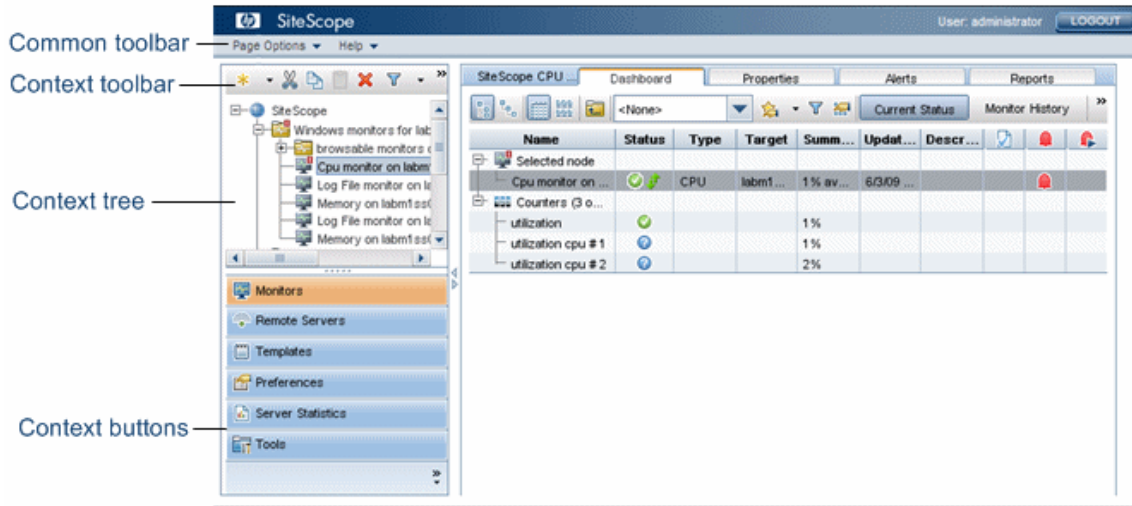
- ▶ Understanding the SiteScope User Interface on page 56
- ▶ Navigating and Performing Actions in the Context Tree on page 60
- ▶ Performing Actions on Multiple Groups and Monitors on page 60
- ▶ Copying and Moving SiteScope Objects on page 61

#### **Reference**

- ▶ SiteScope Keyboard Shortcuts on page 63
- ▶ Navigating SiteScope User Interface on page 64

## Understanding the SiteScope User Interface

When you connect to a SiteScope, the SiteScope opens to the Dashboard view as shown below. If you entered a user name to log on to SiteScope, it is displayed on the upper-right side of the window.



The SiteScope window contains the following key elements:

- ▶ **SiteScope common toolbar.** Provides access to page options, documentation, and additional resources. This toolbar is located on the upper part of the window. For more details, see “SiteScope Common Toolbar” on page 58.
- ▶ **SiteScope context toolbars.** Contains buttons for frequently-used commands in the selected SiteScope context. For more details, see “Tree Toolbar Buttons” on page 65.



- ▶ **SiteScope context tree.** Enables you to create and manage SiteScope objects in a tree structure. For details, see “Monitor Tree” on page 72, “Remote Server Tree” on page 83, and “Template Tree” on page 84.
- ▶ **SiteScope context buttons.** Provide access to the SiteScope Monitors, Remote Servers, Templates, Preferences, Server Statistics, and Diagnostic Tools. For more details, see “SiteScope Context Buttons” on page 59.

---

**Note:** The SiteScope Classic interface, that was available in earlier SiteScope versions using the URL `http://<sitescope_host>:8888`, is no longer available for managing SiteScope. For more information, see “SiteScope Classic Interface” in the *HP SiteScope Deployment Guide* PDF.





---

This section includes the following topics:

- ▶ “SiteScope Common Toolbar” on page 58
- ▶ “SiteScope Context Buttons” on page 59

## SiteScope Common Toolbar

The SiteScope common toolbar, located at the top of the SiteScope window, is accessible from all contexts, and contains the following buttons:


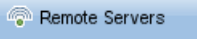

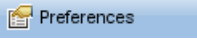


GUI Element	Description
	Enables you to select the following page options: <ul style="list-style-type: none"> <li>▶ <b>Add to Favorites.</b> Enables you to add the current SiteScope view to your list of Favorites in your browser.</li> <li>▶ <b>Save Layout to User Preferences.</b> Enables you to save the current view as the default layout for the specific SiteScope user.</li> </ul>
	Enables you to access SiteScope Help, context-sensitive help for specific windows, release notes, and other additional online resources.  You can also see descriptions of user interface elements in most pages or dialog boxes. To activate this feature, click the <b>Quick Help</b>  button in the specific page or dialog box, and rest the mouse pointer on the element label to display a ToolTip description. Click the <b>Quick Help</b> button again to make this feature unavailable.
	Logs you out of your SiteScope session.

You can customize your view of the monitor tree to list only those SiteScope elements with which you are working. You can also assign search/filter tags to your groups, monitors, reports, and alerts to further refine your selection. For details on this topic, see “Searching and Filtering SiteScope Objects Overview” on page 105.

SiteScope enables you to change monitor configurations across multiple monitors, groups, or multiple SiteScopes using Global Replace. For details on the Global Replace user interface, see “Global Search and Replace Wizard” on page 178.

## SiteScope Context Buttons

SiteScope has the following contexts that are available from the left pane:

GUI Element	Description
	<p>Enables you to create and manage SiteScope groups and monitors in a hierarchy represented by a monitor tree. For details on the user interface, see “Monitor Tree” on page 72.</p>
	<p>Enables you to set up the connection properties so that SiteScope can monitor systems and services running in remote Windows and UNIX environments. For details on the user interface, see “Remote Server Tree” on page 83.</p>
	<p>Enables you to use templates to deploy a standardized pattern of monitoring to multiple elements in your infrastructure. You can use preconfigured SiteScope solution template or create and manage your own templates. For details on the user interface, see “Template Tree” on page 84.</p>
	<p>Enables you to configure specific properties and settings related to most of the administrative tasks within SiteScope. For details on the user interface, see “Preferences Menu” on page 93.</p>
	<p>Enables you to view key SiteScope server performance metrics. For details on the user interface, see “Server Statistics Menu” on page 95.</p>
	<p>Displays diagnostic tools that can help you troubleshoot problems in SiteScope and facilitate monitor configuration. For details on the available tools, see “SiteScope Tools Overview” on page 193.</p>

## **Navigating and Performing Actions in the Context Tree**

There are several ways to navigate the context tree, perform actions, and edit object properties.

You can perform actions using the context toolbar, or you can highlight any object within the context tree itself, and right-click the object to access a menu of options for that object. For example, if you right-click the SiteScope node in the monitor tree, you select from a menu listing only those actions that can be performed on the SiteScope node. You can also perform actions on multiple groups and monitors. For details, see “Performing Actions on Multiple Groups and Monitors” on page 60.

For details of the context tree objects and various context menu options that are available for each object in the tree, see “Monitor Tree” on page 72, “Remote Server Tree” on page 83, “Template Tree” on page 84, “Preferences Menu” on page 93, “Server Statistics Menu” on page 95, and “Tools Menu” on page 97.

## **Performing Actions on Multiple Groups and Monitors**

You can perform mass operations on SiteScope objects using the Manage Groups and Monitors feature. It enables you to perform move, copy, delete, run monitors, enable/disable monitors, and enable/disable associated alert actions on multiple SiteScope objects in the monitor tree. You can also use the Filter options to create a filtered list of groups and monitors based on a filter criteria.

Using the Manage Monitors and Groups dialog box, you can select one or more groups and monitors from an expandable hierarchical view of the organization, and select the action you want to perform.

For details on the user interface, see “Manage Monitors and Groups Dialog Box” on page 68.

## Copying and Moving SiteScope Objects

You can copy SiteScope objects to different locations within a context tree. In addition, you can copy SiteScope objects to templates. You can also move monitors and groups, together with their contents, to different groups in the monitor tree.


To enable you to differentiate between objects, object names must be unique within the parent container. For instance, when you copy or move SiteScope objects, you cannot create two monitors within the same group with exactly the same name. If you make a copy of a SiteScope object and it has the same name as an existing object in the container, SiteScope automatically adds a suffix (number) to the end of the object's name. For example, if you create a copy of monitor Mail Flow and paste it in the same monitor group, SiteScope automatically renames it Mail Flow(1).

You can copy or move the following SiteScope objects:

SiteScope Object	Action and Description
Group	<p><b>Copy/Paste.</b> Copy a monitor group, including its subgroups, monitors, alerts, and reports, to the same or a different monitor group.</p> <p><b>Cut/Paste.</b> Move a monitor group, including its subgroups, monitors, alerts, and reports, to a different monitor group.</p> <p><b>Copy to Template.</b> Copy a monitor group, including its monitors, alerts, and reports, to a template.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ You cannot move or copy a monitor group to its subgroup.</li> <li>▶ If you move a group that is targeted by an alert or report without also moving the alert or report, the group is removed from the alert or report target.</li> <li>▶ Baseline thresholds are not copied or moved with a monitor whose thresholds were set using the baseline.</li> </ul>

SiteScope Object	Action and Description
Monitor	<p><b>Copy/Paste.</b> Copy a monitor, including its alerts and reports, to the same or a different monitor group.</p> <p><b>Cut/Paste.</b> Move a monitor, including its alerts and reports, to a different monitor group.</p> <p><b>Copy to Template.</b> Copy a monitor, including its alerts and reports, to a template.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ If you move a monitor that is targeted by an alert or report without also moving the alert or report, the monitor is removed from the alert or report target.</li> <li>▶ Baseline thresholds are not copied or moved with a monitor whose thresholds were set using the baseline.</li> </ul>
Remote Server	<p><b>Copy to Template.</b> Copy a remote server profile to a template.</p>
Template Container	<p><b>Paste.</b> Paste a template into the template container.</p>
Template	<p><b>Copy/Paste.</b> Copy a template including its groups, monitors, alerts, and report, to a template container.</p>
Template Group	<p><b>Copy/Paste.</b> Copy a template group including its subgroups, monitors, alerts, and reports to a template (provided the template does not already contain a template group) or to a template group.</p>
Template Monitor	<p><b>Copy/Paste.</b> Copy a template monitor including its alerts and reports to a template group.</p>
Alert	<p><b>Copy/Paste.</b> Copy an alert definition (from the Alerts tab) to the same or a different location (group or monitor) in the monitor tree or template tree.</p>
Report	<p><b>Copy/Paste.</b> Copy a report definition (from the Reports tab) to the same or a different location (group or monitor) in the monitor tree or template tree.</p>

---

**Note:** You can also move or copy multiple monitors and groups to a target group by clicking the **Manage Monitors and Groups** button  in the monitor tree toolbar. For details on the user interface, see “Manage Monitors and Groups Dialog Box” on page 68.

---

For details on copying or moving SiteScope objects, expand the context menu option for the relevant SiteScope view in “Navigating SiteScope User Interface” on page 64.

## SiteScope Keyboard Shortcuts

You can perform the following commands in the monitor tree, template tree, and remote server tree by pressing the corresponding shortcut keys:

GUI Element	Description
CTRL+A	Opens the New Alert dialog box, enabling you to create a new alert. For details on the user interface, see “New/Edit Alert Dialog Box” on page 1999.
CTRL+C	Copies the selected item and puts it on the Clipboard.
CTRL+D	Deletes the selected item.
CTRL+F	Opens the New Filter dialog box, enabling you to create a new filter. For details on the user interface, see “New/Edit Filter Dialog Box” on page 111.
CTRL+G	Opens the New Group dialog box, enabling you to create a new group. For details on the user interface, see “New SiteScope Group Dialog Box” on page 297.

GUI Element	Description
CTRL+J	Opens the Select Template/Group dialog box, enabling you to select the template that you want to deploy or the group to which you want to deploy a template. For details on the Select Template user interface, see “Select Template Dialog Box” on page 378. For details on the Select Group user interface, see “Select Group Dialog Box” on page 1636.
CTRL+M	Opens the New Monitor Page, enabling you to add a new monitor. For details on the user interface, see “New Monitor Page” on page 351.
CTRL+R	Clears the filter configured in the Filter dialog box. For details on the user interface, see “New/Edit Filter Dialog Box” on page 111.
CTRL+V	Pastes the contents of the Clipboard to the selected location.
CTRL+X	Cuts the selected item and puts it on the Clipboard.
DELETE	Deletes the selection.
F5	Refreshes the tree.

## Navigating SiteScope User Interface

**This section includes:**

- ▶ Tree Toolbar Buttons on page 65
- ▶ Manage Monitors and Groups Dialog Box on page 68
- ▶ Monitor Tree on page 72
- ▶ Remote Server Tree on page 83
- ▶ Template Tree on page 84
- ▶ Preferences Menu on page 93
- ▶ Server Statistics Menu on page 95
- ▶ Tools Menu on page 97













- Alerts Tab Context Menu Options on page 101
- Reports Tab Context Menu Options on page 102



## Tree Toolbar Buttons

<b>Description</b>	Enables you to perform common functions in the different SiteScope views. Some toolbar buttons are not available in all SiteScope views.
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Monitor Tree” on page 72</li> <li>➤ “Remote Server Tree” on page 83</li> <li>➤ “Template Tree” on page 84</li> </ul>


The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click the <b>New</b> button to add SiteScope objects (groups, monitor, alerts, remote servers, and templates) to the relevant tree. The objects that you can add depend on the context.
	Click the <b>Test</b> button to test the connection to the server. <b>Note:</b> Available in the remote server tree toolbar only.
	Click the <b>Detailed Test</b> button to run a test that displays the result of running commands on the remote server. This enables checking the permissions for the defined user. <b>Note:</b> Available in the remote server tree toolbar for UNIX servers only.
	Click the <b>Cut</b> button to move the selected object to another location in the tree.
	Click the <b>Copy</b> button to make a copy of the selected object.




GUI Element	Description
	<p>Click the <b>Paste</b> button to copy or move an object to the selected location in the tree.</p>
	<p>Click the <b>Delete</b> button to delete the selected object from the tree.</p>
	<p>Enables you to filter the monitor tree to display only those SiteScope objects that meet the criteria that you define.</p> <p>Click the <b>Filter</b> button and select a filter option:</p> <ul style="list-style-type: none"> <li>▶ <b>New Filter.</b> Opens the New Filter dialog box which enables you to create a filter. For details on the user interface, see “New/Edit Filter Dialog Box” on page 111.</li> <li>▶ <b>Clear Filter.</b> Clears the filter settings.</li> <li>▶ <b>&lt;List of existing filters&gt;.</b> Displays a list of existing filters. The following options are available: <ul style="list-style-type: none"> <li>▶ <b>Apply.</b> Applies the filter to the left tree pane.</li> <li>▶ <b>Edit.</b> Opens the Edit Filter dialog box which enables you to edit the filter. For details on the user interface, see “New/Edit Filter Dialog Box” on page 111.</li> <li>▶ <b>Delete.</b> Deletes the filter from the filter list.</li> </ul> </li> </ul> <p><b>Note:</b> Available in the monitor tree toolbar only.</p>
	<p>Click the <b>Refresh</b> button to refresh the data in the tree.</p>
	<p>Click the <b>Manage Monitors and Groups</b> button to perform an action (copy, move, delete, run monitors, enable/disable monitors, enable/disable associated alerts) on multiple groups and monitors in the monitor tree. You can also filter the list of objects in the monitor tree. For details on the Manage Monitors and Groups dialog box, see “Manage Monitors and Groups Dialog Box” on page 68.</p> <p><b>Note:</b> Available in the monitor tree toolbar only.</p>






GUI Element	Description
	<p>Click the <b>Show/Hide Pane</b> buttons to show or hide the tree, and expand or contract the right pane.</p>
	<p>Click to configure the context button display. The following options are available:</p> <ul style="list-style-type: none"> <li>▶ <b>Show More Buttons.</b> Click to show the next highest ranking SiteScope context button in the left pane. This button is available only if not all the context buttons are displayed.</li> <li>▶ <b>Show Fewer Buttons.</b> Click to hide the lowest ranking SiteScope context button from the left pane. This button is available only if at least one context buttons is displayed.</li> <li>▶ <b>Option.</b> Choose the order in which the SiteScope context buttons are displayed. Use the <b>Move Up</b> and <b>Move Down</b> buttons to rearrange the order. To hide a button from the left pane, clear the check box for the context. By default, all the context buttons are selected (displayed in the left pane).</li> <li>▶ <b>Add or Remove Buttons.</b> Shows the show/hide status of the context buttons. By default, all the context buttons are selected (displayed in the left pane). To hide a button, clear the check box for the context.</li> </ul>



## **Manage Monitors and Groups Dialog Box**

<b>Description</b>	<p>Enables you to select one or more groups, monitors, or both, and perform an action on the selected objects (copy, move, delete, run monitors, enable/disable monitors, enable/disable associated alerts). You can also use the filter options to create a filtered list of groups and monitors based on a filter criteria, or select an existing filter previously defined in the monitor tree filter.</p> <p><b>To access:</b> In the monitor or template tree toolbar, click the <b>Manage Monitors and Groups</b>  button.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The toolbar actions are available according to the user permissions and the objects selected.</li> <li>▶ The Health container cannot be deleted.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Manage a Group – Workflow” on page 294</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> <li>▶ “Create and Define a New Search/Filter Tag” on page 108</li> </ul>
<b>Useful Links</b>	<p>“Performing Actions on Multiple Groups and Monitors” on page 60</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Enables you to filter the monitor tree to display only those SiteScope objects that meet the criteria that you define. After applying a filter, the name of the filter is displayed in the button (<b>custom</b>, if the filter was created in the Manage Monitors and Groups dialog box; otherwise the name of the filter defined in the monitor tree filter).</p> <p>Click the <b>Filter</b> button arrow and select a filter option:</p> <ul style="list-style-type: none"> <li>▶ <b>New Filter.</b> Opens the New Filter dialog box which enables you to create a filter. For details on the user interface, see “New/Edit Filter Dialog Box” on page 111.</li> <li>▶ <b>Clear Filter.</b> Clears the filter settings.</li> <li>▶ <b>&lt;List of existing filters&gt;.</b> Displays a list of existing filters previously defined in the monitor tree filter.</li> </ul>
	<p>Click the <b>Select All</b> button to select all listed SiteScope objects.</p>
	<p>Click the <b>Clear Selection</b> button to clear the selection.</p>

GUI Element	Description
	<p>Click the <b>Cut</b> button to move the selected objects to the destination group.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ Any alerts defined for a specific monitor are transferred with the monitor.</li> <li>▶ Moving a monitor restarts its history and any reports generated for the monitor are started from the time that the monitor was moved. The history data is still in the log files, but it is inaccessible from the reports for the monitor after it has been moved. Moving groups has no effect on history.</li> <li>▶ Moving a monitor may break group-to-monitor dependencies. If you have one or more groups dependent on the status of the monitor you are moving, you should update that dependency after moving the monitor.</li> </ul>
	<p>Click the <b>Copy</b> button to make a copy of the selected objects for pasting to the destination group.</p>
	<p>Click the <b>Paste</b> button to paste the selected objects to the destination group. If you make a copy of a SiteScope object and it has the same name as an existing object in the container, SiteScope automatically adds a suffix (number) to the end of the object's name.</p> <p><b>Example:</b> If you create a copy of monitor Mail Flow and paste it in the same monitor group, SiteScope automatically renames it Mail Flow(1).</p>
	<p>Click the <b>Delete</b> button to delete the selected objects from the monitor tree.</p>
	<p>Click the <b>Run Monitors</b> button to run the monitor or any monitors configured in the group. This opens an information window with the results.</p>

GUI Element	Description
	<p>Click the <b>Enable/Disable Monitor</b> button to open the Enable/Disable Monitor dialog box which enables you to enable or disable the monitor or all the monitors in the group, regardless of the setting in the monitor properties. If you select <b>Disable</b>, the monitors are disabled until you return to this dialog box and select <b>Enable</b>. For details on the user interface, see “Enable/Disable Monitor or Monitors in Group Dialog Box” on page 1879.</p>
	<p>Click the <b>Enable/Disable Associated Alerts</b> button to open the Enable/Disable Associated Alerts dialog box which enables you to enable or disable all alerts associated with the monitor or all monitors in the group. For more details, see “Enable/Disable Associated Alerts” on page 374.</p>
<p>&lt;SiteScope objects&gt;</p>	<p>Actions are applied to all monitors and groups that are selected using the check box selections in the tree. The display of the tree is saved across visits to the dialog box and the actions associated with it.</p> <ul style="list-style-type: none"> <li>➤ To select an object, select the check box to the left of the object name. Any combination of groups or monitors can be selected. A <input type="checkbox"/> icon displayed to the left of a group indicates that not all monitors and subgroups contained within that group have been selected.</li> <li>➤ To select a destination for copying or moving an object, click the object name (not the check box).</li> </ul> <p><b>Default value:</b> The top level groups are shown, but no objects are selected.</p>





## Monitor Tree





<b>Description</b>	<p>Represents the organization of systems and services in your network environment. The tree includes containers and objects within your infrastructure.</p> <p>The Context Menu Options include descriptions of the various context menu options that are available for each object in the monitor tree.</p>
<b>Important Information</b>	<ul style="list-style-type: none"><li>▶ The root node of the tree is the SiteScope container. Only one SiteScope node exists in the monitor tree. You add all other elements to the tree under the SiteScope node.</li><li>▶ You can search for objects in the monitor tree by selecting a node and typing the characters you want to search in the popup search box. Click the ESC key to close the search box.</li></ul>
<b>Useful Links</b>	<p>“Working with SiteScope Monitors” on page 301</p>



## Monitor Tree Objects

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
 SiteScope	<p>Represents an individual SiteScope server.</p> <p><b>Parent:</b> Enterprise node or container.</p> <p><b>Add to tree by:</b> Importing or adding an empty SiteScope profile.</p>
	<p>Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors).</p> <p>If an alert has been set up for the monitor group or subgroup, the alert  symbol is displayed next to the group icon.</p> <p>If a Management report has been set up for the monitor group or subgroup, the report  symbol is displayed next to the group icon.</p> <p><b>Parent:</b> SiteScope or SiteScope group.</p> <p><b>Add to tree by:</b> Creating, or importing with a SiteScope that has groups defined.</p>

GUI Element	Description
	<p>Represents a SiteScope monitor (enabled/disabled).</p> <p>If an alert has been set up for the monitor, the alert  symbol is displayed next to the monitor icon.</p> <p>If a Management report has been set up for the monitor, the report  symbol is displayed next to the monitor icon.</p> <p><b>Parent:</b> SiteScope group or subgroup, template, or solution template.</p> <p><b>Add to tree by:</b> Creating, or importing with a SiteScope that has monitors configured.</p>
	<p>Represents the collection of available health monitors that are deployed to check proper functioning of SiteScope monitors.</p> <p><b>Parent:</b> SiteScope.</p> <p><b>Add to tree by:</b> Automatically added with SiteScope object.</p>

## SiteScope Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Baselining</b>	<p>Enables you to create a baseline for monitoring variations in response times and performance in the infrastructure for all monitors under SiteScope.</p> <ul style="list-style-type: none"> <li>▶ <b>Calculate.</b> Enables you to select monitors and specify the relevant time and schedule to be used for calculating the baseline. It also enables you to select and fine-tune the baseline adherence level and define boundaries.</li> <li>▶ <b>Review &amp; Activate.</b> Displays a summary of calculated monitors and baseline data. It also enables you to save the current monitor configuration, view and retry failed operations, view baseline measurement graphs, and apply the baseline configuration.</li> <li>▶ <b>Remove.</b> Enables you to remove the baseline threshold or recalculate the baseline after a baseline has been calculated.</li> <li>▶ <b>Status Report.</b> Displays information about the baseline status for all monitors under SiteScope.</li> </ul> <p>For details on this topic, see “Setting Status Thresholds Using a Baseline” on page 312.</p>
<b>Deploy Template</b>	<p>Opens the Select Template dialog box that enables you to select a template to deploy to the group. For details on the user interface, see “Select Template Dialog Box” on page 378.</p>
<b>Deploy Template Using CSV</b>	<p>Opens the Select Template dialog box which enables you to select a template to deploy to the group using a CSV file. For details on the user interface, see “Select Template Dialog Box” on page 378.</p>
<b>Expand All</b>	<p>Opens all the subtrees under SiteScope.</p>

Menu Item (A-Z)	Description
<b>Global Search and Replace</b>	Opens the Global Search and Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details on this topic, see “Global Search and Replace Wizard” on page 178.
<b>Monitor Deployment Wizard</b>	This menu item is available only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center. Opens the Monitor Deployment Wizard. For details on this topic, see “Monitor Deployment Wizard” on page 1811.
<b>New &gt; Alert</b>	Opens the New Alert window which enables you to define a new alert for SiteScope. For details on this topic, see “SiteScope Alerts” on page 1959.
<b>New &gt; Group</b>	Opens the New Group window which enables you to define a new SiteScope group. For details on the user interface, see “New SiteScope Group Dialog Box” on page 297.
<b>Paste</b>	Pastes the selected SiteScope object (that was previously copied or cut) to the SiteScope node.
<b>Paste from other SiteScope</b>	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Pastes the selected SiteScope object (that was previously copied or cut) from another SiteScope to the SiteScope node.
<b>Reports &gt; Management/Quick/Monitor/Alert</b>	Enables you to select the type of SiteScope report you want to define. For details on these reports, see “SiteScope Reports” on page 2035.
<b>Reports &gt; BAC Configuration Changes</b>	This menu item is available only through System Availability Management Administration when the SiteScope is connected to Business Availability Center. Displays a log of configuration changes made to Business Availability Center. For details, see “SiteScope Report Types” on page 2037.

## Group Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Baselining</b>	<p>Enables you to create a baseline for monitoring variations in response times and performance in the infrastructure for all monitors in the group.</p> <ul style="list-style-type: none"> <li>▶ <b>Calculate.</b> Enables you to select monitors from the group and specify the relevant time and schedule to be used for calculating the baseline. It also enables you to select and fine-tune the baseline adherence level and define boundaries.</li> <li>▶ <b>Review &amp; Activate.</b> Displays a summary of calculated monitors and baseline data for the group. It also enables you to save the current monitor configuration, view and retry failed operations, view baseline measurement graphs, and apply the baseline configuration.</li> <li>▶ <b>Remove.</b> Enables you to remove the baseline threshold or recalculate the baseline after a baseline has been calculated.</li> <li>▶ <b>Status Report.</b> Displays information about the baseline status for all monitors in the group.</li> </ul> <p>For details on this topic, see “Setting Status Thresholds Using a Baseline” on page 312.</p>
<b>Copy</b>	<p>Copies the group and its contents (monitors, alerts, and reports) to a monitor group or template.</p> <p><b>Note:</b> When copying a group that contains monitors with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitors are no longer in baseline mode.</p>

Menu Item (A-Z)	Description
<b>Copy to other SiteScope</b>	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Copies the group and its contents (monitors, alerts, and reports) from another SiteScope to a monitor group or template in the SiteScope node.
<b>Copy to Template</b>	Copies the group and its contents (monitors, alerts, and reports) to a template group. For details on this topic, see “Create a Template by Copying Existing Configurations” on page 1586.
<b>Cut</b>	<p>Moves the group and its contents (monitors, alerts, and reports) or a monitor and its contents (alerts and reports) to a monitor group.</p> <p><b>Note:</b> When moving a group that contains monitors with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitors are no longer in baseline mode.</p>
<b>Delete</b>	<p>Deletes the group.</p> <p><b>Note:</b> You cannot delete a group if it has dependent alerts or reports at the container level. To delete a group with dependencies, you must remove the group from <b>Alert Targets</b> and <b>Report Targets</b> for each dependency, and then delete the group. You can delete groups that have dependencies at the child level.</p>
<b>Deploy Template</b>	Opens the Select Template dialog box that enables you to select a template to deploy to the group. For details on the user interface, see “Select Template Dialog Box” on page 378.
<b>Deploy Template Using CSV</b>	Opens the Select Template dialog box which enables you to select a template to deploy to the group using a CSV file. For details on the user interface, see “Select Template Dialog Box” on page 378.
<b>Expand All</b>	Opens all the subtrees under the group.

Menu Item (A-Z)	Description
<b>Global Search and Replace</b>	Opens the Global Search and Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details on this topic, see “Global Search and Replace Wizard” on page 178.
<b>Monitor Deployment Wizard</b>	This menu item is available only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center. Opens the Monitor Deployment Wizard. For details on this topic, see “Monitor Deployment Wizard” on page 1811.
<b>New &gt; Alert</b>	Opens the New Alert window which enables you to define a new alert for the group. For details on this topic, see “SiteScope Alerts” on page 1959.
<b>New &gt; Group</b>	Opens the New Group window which enables you to define a new SiteScope group. For details on the user interface, see “New SiteScope Group Dialog Box” on page 297.
<b>New &gt; Monitor</b>	Opens the New Monitor window which enables you to define a new SiteScope monitor. For details on the user interface, see “New Monitor Page” on page 351.
<b>Paste</b>	Pastes the selected group and its contents (monitors, alerts, and reports) or a monitor and its contents (alerts and reports) to the specified monitor group.
<b>Paste from other SiteScope</b>	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Pastes the selected group and its contents (monitors, alerts, and reports) or a monitor and its contents (alerts and reports) from another SiteScope to the specified monitor group.
<b>Reports</b>	Enables you to select the type of SiteScope report you want to define. For details on this topic, see “SiteScope Reports” on page 2035.
<b>Run Monitors</b>	Runs any monitors configured in the group, and opens an information window with the results.

## Monitor Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Baselining</b>	<p>Enables you to create a baseline for monitoring variations in response times and performance in the infrastructure for the specific monitor.</p> <ul style="list-style-type: none"> <li>▶ <b>Calculate.</b> Enables you to select the monitor and specify the relevant time and schedule to be used for calculating the baseline. It also enables you to select and fine-tune the baseline adherence level and define boundaries.</li> <li>▶ <b>Review &amp; Activate.</b> Displays a summary of the calculated monitor's baseline data. It also enables you to save the current monitor configuration, view and retry failed operations, view baseline measurement graphs, and apply the baseline configuration.</li> <li>▶ <b>Remove.</b> Enables you to remove the baseline threshold or recalculate the baseline after a baseline has been calculated.</li> <li>▶ <b>Status Report.</b> Displays information about the monitor's baseline status.</li> </ul> <p>For details on this topic, see "Setting Status Thresholds Using a Baseline" on page 312.</p>
<b>Copy</b>	<p>Copies the monitor and its contents (alerts and reports) to a monitor group or template.</p> <p><b>Note:</b> When copying a monitor with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitor is no longer in baseline mode.</p>
<b>Copy to other SiteScope</b>	<p>This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Copies the monitor and its contents (alerts and reports) from another SiteScope to a monitor group or template.</p>



Menu Item (A-Z)	Description
<b>Copy to Template</b>	Copies the monitor and its contents (alerts and reports) to a template group. For details on this topic, see “Create a Template by Copying Existing Configurations” on page 1586.
<b>Cut</b>	Moves the monitor and its contents (alerts and reports) to a monitor group. <b>Note:</b> When moving a monitor with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitor is no longer in baseline mode.
<b>Delete</b>	Deletes the monitor. <b>Note:</b> You cannot delete a monitor if it has dependent alerts or reports at the container level. To delete a monitor with dependencies, you must remove the monitor from <b>Alert Targets</b> and <b>Report Targets</b> for each dependency, and then delete the monitor. You can delete monitors that have dependencies at the child level.
<b>Global Search and Replace</b>	Opens the Global Search and Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details on this topic, see “Global Search and Replace Wizard” on page 178.
<b>New &gt; Alert</b>	Opens the New Alert window which enables you to define a new alert for the monitor. For details on this topic, see “SiteScope Alerts” on page 1959.
<b>Paste</b>	Pastes the selected monitor context object to the specified monitor.
<b>Paste from other SiteScope</b>	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Pastes the selected monitor context object from another SiteScope to the specified monitor.
<b>Reports</b>	Enables you to select the type of SiteScope report you want to define. For details on this topic, see “SiteScope Reports” on page 2035.

Menu Item (A-Z)	Description
<b>Run Monitor</b>	Runs the monitor and opens an information window with the results.

### SiteScope Health Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):



Menu Item (A-Z)	Description
<b>Disable Logging</b>	Disables logging on SiteScope Health. For details, see “SiteScope Server Health” on page 1895.
<b>Enable Logging</b>	Enables logging on SiteScope Health. For details, see “SiteScope Server Health” on page 1895.
<b>Expand All</b>	Opens all the subtrees under SiteScope Health.
<b>New &gt; Alert</b>	Opens the New Alert window which enables you to define a new alert for Health. For details on this topic, see “SiteScope Alerts” on page 1959.
<b>New &gt; Group</b>	Opens the New Group window which enables you to define a new SiteScope group. For details on the user interface, see “New SiteScope Group Dialog Box” on page 297.
<b>New &gt; Monitor</b>	Opens the New Monitor window which enables you to define a new SiteScope monitor. For details on the user interface, see “New Monitor Page” on page 351.
<b>Paste</b>	Pastes monitors and monitor groups into the Health container.
<b>Recreate missing health monitors</b>	Enables you to restore health monitors that have been deleted from the <b>Health</b> container.
<b>Reports</b>	Enables you to select the type of SiteScope report you want to define. For details on this topic, see “SiteScope Reports” on page 2035.
<b>Run Monitors</b>	Runs the health monitors and opens an information window with the results.

## Remote Server Tree

<b>Description</b>	Represents the remote servers configured in your network environment.  The Context Menu Options include descriptions of the various context menu options that are available for each object in the remote server tree.
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Working with Remote Servers” on page 1275</li> <li>▶ “Remote Server Properties Page” on page 1288</li> </ul>

### Remote Server Tree Objects

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Represents the Windows/UNIX remote server container in the remote server view.
	Represents a Windows/UNIX remote server. <b>Parent:</b> Windows/UNIX Remote Server container. <b>Add by:</b> Creating in the Windows/UNIX Remote Server container or template tree.

### Remote Servers Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>New Microsoft Windows/UNIX Remote Server</b>	Opens the New Server window which enables you to define a new Microsoft Windows or UNIX server.

## Remote Server Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):





Menu Item (A-Z)	Description
<b>Copy to Template</b>	Copies the remote server to a template group. For details on this topic, see “Create a Template by Copying Existing Configurations” on page 1586.
<b>Delete</b>	Deletes the remote server
<b>Detailed Test (for UNIX servers only)</b>	Enables you to test the running commands on the remote host and check the permissions for the defined user. Available for UNIX servers only.
<b>Test</b>	Enables you to test the connection to the remote server.









## Template Tree

<b>Description</b>	<p>Represents the SiteScope solution template sets, template examples, Monitor Deployment Wizard templates, and user-defined templates that are available for deployment to monitor groups.</p> <p>The Context Menu Options include descriptions of the various context menu options that are available for each object in the template tree.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Templates” on page 1557</li> <li>➤ “SiteScope Solution Templates” on page 1665</li> <li>➤ “SiteScope Templates Page” on page 1605</li> <li>➤ “Templates Tree - Alerts Tab” on page 1607</li> </ul>

## Template Tree Objects

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
 SiteScope	Represents an individual SiteScope server. <b>Parent:</b> Enterprise node or container. <b>Add to tree by:</b> Importing or adding an empty SiteScope profile.
	Represents a solution template container (available/unavailable). Only licensed solution templates that have the available icon are configurable solution templates. <b>Parent:</b> SiteScope.
	Represents a template container. A template container is used to organize configuration deployment templates. <b>Parent:</b> SiteScope. <b>Add to template tree by:</b> Creating, or importing with a SiteScope that has template containers defined.
	Represents a template configuration for deploying SiteScope objects. <b>Parent:</b> Template container. <b>Add to template tree by:</b> Creating.

GUI Element	Description
	<p>Represents a SiteScope template group or subgroup (with enabled monitors/with no monitors or no enabled monitors).</p> <p>If an alert has been set up for the template group or subgroup, the alert  symbol is displayed next to the group icon.</p> <p>If a Management report has been set up for the template group or subgroup, the report  symbol is displayed next to the group icon.</p> <p><b>Parent:</b> Template.</p> <p><b>Add to tree by:</b> Creating, or importing with a SiteScope that has template groups defined.</p>
	<p>Represents a SiteScope template monitor (enabled/disabled).</p> <p>If an alert has been set up for the template monitor, the alert  symbol is displayed next to the monitor icon.</p> <p>If a Management report has been set up for the template monitor, the report  symbol is displayed next to the monitor icon.</p> <p><b>Parent:</b> Template group or subgroup, template, or solution template.</p> <p><b>Add to tree by:</b> Creating, or importing with a SiteScope that has template monitors configured.</p>
	<p>Represents a Windows/UNIX remote server.</p> <p><b>Parent:</b> Template.</p> <p><b>Add by:</b> Creating in the remote server tree or template tree.</p>
	<p>Represents a variable used as placeholder to prompt for input when deploying a template.</p> <p><b>Parent:</b> Template.</p> <p><b>Add to template tree by:</b> Creating.</p>

## SiteScope Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Expand All</b>	Opens all the subtrees under SiteScope.
<b>New &gt; Template Container</b>	Opens the New Template Container window which enables you to define a new template container.

## Solution Templates Container Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Expand All</b>	Expands the solution templates container to display all the solution templates within the container.

## Solution Template Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Copy</b>	Copies a solution template. You can paste the solution template to a template container in the template tree.
<b>Deploy Template</b>	Opens the Select Group dialog box which enables you to select the group to which to deploy the solution template. For details on the user interface, see “Select Group Dialog Box” on page 1636.
<b>Deploy Template Using CSV</b>	Opens the Select Group dialog box which enables you to select the group to which to deploy the template using a CSV file. For details on the user interface, see “Select Group Dialog Box” on page 1636.

Menu Item (A-Z)	Description
<b>Expand All</b>	Expands the solution templates container to display all the solution templates within the container.
<b>Generate XML</b>	Opens the Generate Auto Deployment XML window which enables you to create an XML file to use for automatically deploying the solution template. For details on the topic, see “Auto Template Deployment” on page 1643. For details on the user interface, see “Generate Auto Deployment XML” on page 1640.

### Template Container Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Delete</b>	Deletes the template container.
<b>Expand All</b>	Expands the templates container to display all the template objects within the container.
<b>Export</b>	Opens the Export Template window which enables you to export a template file.
<b>Generate XML</b>	Opens the Generate Auto Deployment XML window which enables you to create an XML file to use for automatically deploying the templates in the container.
<b>Import</b>	Opens the Import Template window which enables you to import a template file.
<b>New &gt; Template</b>	Opens the New Container window which enables you to define a new template.
<b>New &gt; Template Container</b>	Opens the New Template Container window which enables you to define a new template container.
<b>Paste</b>	Pastes a template into the template container.



## Template Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Copy</b>	Copies a template group, monitor, or alert. You can paste the template group, monitor, or alert to the SiteScope tree.
<b>Delete</b>	Deletes the template.
<b>Deploy Template</b>	Opens the Select Group dialog box which enables you to select the group to which to deploy the template. For details on the user interface, see “Select Group Dialog Box” on page 1636.
<b>Deploy Template Using CSV</b>	Opens the Select Group dialog box which enables you to select the group to which to deploy the template using a CSV file. For details on the user interface, see “Select Group Dialog Box” on page 1636.
<b>Expand All</b>	Opens all the subtrees under the template.
<b>New &gt; Group</b>	<p>Opens the New Group window, which enables you to define a new template group. For details on the user interface, see “New SiteScope Group Dialog Box” on page 297.</p> <p><b>Note:</b> This menu item is available only if the template does not already contain a template group.</p>
<b>New &gt; UNIX Server</b>	<p>Opens the New Template window, which enables you to define a new remote UNIX template.</p> <p><b>Note:</b> This menu item is available only if the template does not already contain a remote server.</p>

Menu Item (A-Z)	Description
<b>New &gt; Variable</b>	Opens the New Template Variable window, which enables you to define a new template variable.
<b>New &gt; Microsoft Windows Server</b>	Opens the New Template window, which enables you to define a new remote NT template. <b>Note:</b> This menu item is available only if the template does not already contain a remote server.
<b>Paste</b>	Pastes a template group, monitor, or alert to a template.
<b>Publish Changes</b>	Opens the Publish Template Changes wizard, which enables you to check deployed groups for template compliancy and to update SiteScope objects deployed by templates whenever the template is updated.

### Template Variable Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Copy</b>	Copies the template variable to a template.
<b>Delete</b>	Deletes the template variable.

### Template Remote Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets):

Menu Item (A-Z)	Description
<b>Copy</b>	Copies the template remote to a template. <b>Note:</b> You can add only one template remote server to a template. This does not apply to templates created in older versions of SiteScope.
<b>Delete</b>	Deletes the template remote.

## Template Group Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Copy</b>	Copies the template group and its contents (monitors, alerts, and subgroups) to a template.
<b>Delete</b>	Deletes the template group.
<b>Expand All</b>	Opens all the subtrees under the template group.
<b>New &gt; Alert</b>	Opens the New Template Alert window which enables you to define a new alert for the template group. For details on this topic, see “SiteScope Alerts” on page 1959.
<b>New &gt; Group</b>	Opens the New Template Group window which enables you to define a new template subgroup. For details on the user interface, see “New SiteScope Group Dialog Box” on page 297.
<b>New &gt; Monitor</b>	Opens the New Monitor window which enables you to define a new SiteScope monitor for the template group. For details on the user interface, see “New Monitor Page” on page 351.
<b>Paste</b>	Pastes the selected template group and its contents (monitors, alerts, and subgroups) to a template.

## Template Monitor Context Menu Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Copy</b>	Copies the template monitor and its contents (alerts) to a template group.
<b>Delete</b>	Deletes the template monitor.
<b>New &gt; Alert</b>	Opens the New Template Alert window which enables you to define a new alert for the template monitor. For details on this topic, see “SiteScope Alerts” on page 1959.
<b>Paste</b>	Pastes the selected template monitor and its contents (alerts) to a template group.

## Preferences Menu

<b>Description</b>	Represents the preference types that enable you to configure specific properties and settings related to most of the administrative tasks available within SiteScope.
<b>Important Information</b>	Only an administrator, or a user granted <b>Edit &lt;preference type&gt;</b> permissions, can create or make changes to SiteScope Preferences.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Preference types>	<p>The following are the preference types in SiteScope:</p> <ul style="list-style-type: none"> <li>▶ <b>General Preferences.</b> Use to perform various post-configuration tasks, such as enter standard and optional SiteScope license keys, control display functions, and set security options. For details, see “General Preferences” on page 1375.</li> <li>▶ <b>Infrastructure Preferences.</b> Use to define the values of global settings that determine how SiteScope runs. For details, see “Infrastructure Preferences” on page 1387.</li> <li>▶ <b>Integration Preferences.</b> Use to configure SiteScope as a data collector for Business Availability Center. For details, see “Integration Preferences” on page 1415.</li> <li>▶ <b>Failover Preferences.</b> Use to indicate a primary SiteScope to be mirrored and set how often the configurations should be mirrored to the SiteScope Failover installation. For details, see “Failover Preferences” on page 1457.</li> <li>▶ <b>Log Preferences.</b> Use to controls the accumulation and storage of monitor data logs. For details, see “Log Preferences” on page 1449.</li> </ul>

GUI Element	Description
<p>&lt;Preference types&gt; (continued)</p>	<ul style="list-style-type: none"> <li>▶ Email Preferences. Use to define email server settings and profiles for SiteScope email alert and status reports. For details, see “Email Preferences” on page 1461.</li> <li>▶ Pager Preferences. Use to configure settings and additional pager profiles that SiteScope uses for sending Pager alerts. For details, see “Pager Preferences” on page 1471.</li> <li>▶ SNMP Trap Preferences. Use to define settings that are used by SiteScope SNMP Trap alerts when sending data to management consoles. For details, see “SNMP Trap Preferences” on page 1481.</li> <li>▶ Schedule Preferences. Use for customizing the operation of SiteScope monitors and alerts to run only at specific times or during specific time periods. For details, see “Schedule Preferences” on page 1487.</li> <li>▶ User Management Preferences. Use to define and manage user login profiles that control how others access SiteScope. For details, see “User Management Preferences” on page 1497.</li> <li>▶ Credential Preferences. Use to create and manage credentials for SiteScope resources. For details, see “Credential Preferences” on page 1523.</li> <li>▶ Search/Filter Tags. Use to manage the Search/Filter tags defined in SiteScope. You can assign tags to one or more items in the context trees and preference profiles, and then use the tags as an object for a filter. For details, see “Search/Filter Tags” on page 1533.</li> <li>▶ Certificate Management. Use to add and remove server certificates and reload the keystore, without having to restart SiteScope after each certificate change operation. For details, see “Certificate Management” on page 1535.</li> </ul>
<p>&lt;Preferences&gt;</p>	<p>Represents a preference.</p> <p><b>Add by:</b> Creating in the specific preference container, or importing with a SiteScope that has preferences defined.</p>

 **Server Statistics Menu**


<b>Description</b>	<p>Enables you to view an overview of several key SiteScope server performance statistics. This includes:</p> <ul style="list-style-type: none"> <li>▶ the load on the SiteScope server</li> <li>▶ a list of currently running and recently run monitors and status data</li> <li>▶ process manager summary and statistics for the perfex pools</li> <li>▶ SSH statistics and connection summary</li> <li>▶ Telnet statistics and connection summary</li> <li>▶ SiteScope log files</li> </ul>
<b>Important Information</b>	<p>Only an administrator, or a user granted <b>View server statistics</b> permissions, can view the monitor performance data pages.</p>
<b>Included in Tasks</b>	<p>“Analyze SiteScope Server Statistics” on page 1930</p>
<b>Useful Links</b>	<p>“Using Server Statistics” on page 1922</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Menu options>	<p>The following are the available monitor performance data options in SiteScope:</p> <ul style="list-style-type: none"> <li>▶ <b>General.</b> Displays SiteScope server statistics, including the load on the SiteScope server (number of running monitors, waiting monitors, monitor runs per minute), and a list of running monitors by type. For details, see “General Page” on page 1944.</li> <li>▶ <b>Running Monitors.</b> Displays a list of which SiteScope monitors are running, and which monitors have run recently, at what time, and what was the returned status. For details, see “Running Monitors Page” on page 1945.</li> <li>▶ <b>Perfex Processes Pool.</b> Displays the process manager summary, and pool statistics and status tables for each pool. For details, see “Perfex Process Pool Page” on page 1947.</li> <li>▶ <b>SSH Connections.</b> Displays Secure Shell (SSH) statistics and a summary of SSH connections when using SSH to connect to remote UNIX or Windows servers. For details, see “SSH Connections Page” on page 1950.</li> <li>▶ <b>Telnet Connections.</b> Displays telnet statistics when using telnet to connect to remote UNIX or Windows servers. For details of the user interface, see “Telnet Connections Page” on page 1952.</li> <li>▶ <b>Log Files.</b> Displays the list of log files in SiteScope that are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions. For details of the user interface, see “Log Files Page” on page 1954.</li> </ul>



 **Tools Menu**

<b>Description</b>	Displays a list of diagnostic tools that can help you troubleshoot problems in SiteScope and facilitate monitor configuration.
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ To view or use the tools in the <b>Tools</b> context in the left pane, you must be an administrator in SiteScope, or a user granted <b>Use tools</b> permissions.</li> <li>▶ Some tools are also available when configuring or editing specific monitors (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). If a tool is available when configuring or editing a monitor, you can access the tool by: <ul style="list-style-type: none"> <li>▶ Clicking the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ Clicking the <b>Tools</b>  button in the SiteScope Dashboard toolbar when running the test tool for an existing monitor. This opens and runs the tool with the monitor's existing data as its input, and displays test results in the <b>Results</b> panel.</li> </ul> </li> <li>▶ To avoid character set problems when the SiteScope client uses a multibyte locale different from the SiteScope server, set the value in the <b>master.config</b> file for the <b>_httpCharset</b> setting to <b>UTF-8</b>. By default, the <b>_httpCharset</b> value is empty, which means that the default server locale is used.</li> </ul>
<b>Useful Links</b>	"SiteScope Tools Overview" on page 193

The following tools are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Application Tools</b>	
<b>Microsoft Windows Media Player Tool</b>	Tests Microsoft Windows Media Player streaming. For more information, see “Microsoft Windows Media Player Tool” on page 218.
<b>News Server Tool</b>	Checks whether a News Server is operational. For more information, see “News Server Tool” on page 221.
<b>Real Media Player Tool</b>	Tests Real Media Player streaming. For more information, see “Real Media Player Tool” on page 230.
<b>Common Utility Tools</b>	
<b>Regular Expression Tool</b>	Tests a regular expression for content matching against a sample of the content you want to monitor. For more information, see “Regular Expression Tool” on page 232.
<b>XSL Transformation Tool</b>	Tests custom XSL transformation of XML data to be monitored with the Browsable XML Monitor. For more information, see “XSL Transformation Tool” on page 258.
<b>Database Tools</b>	
<b>Database Connection Tool</b>	Checks connectivity and configuration of JDBC or ODBC database connections. For more information, see “Database Connection Tool” on page 198.
<b>Database Information Tool</b>	Retrieves and displays database server metadata such as product and driver version, SQL compatibility level information, and supported SQL functions. For more information, see “Database Information Tool” on page 201.
<b>LDAP Authentication Tool</b>	Tests an LDAP server by requesting a user authentication. For more information, see “LDAP Authentication Tool” on page 211.

GUI Element	Description
<b>Mail Tools</b>	
<b>Mail Round Trip Tool</b>	Tests a mail server by sending and retrieving a test message. For more information, see “Mail Round Trip Tool” on page 214.
<b>Network Tools</b>	
<b>DNS Lookup Tool</b>	Tests a DNS server to verify that it can resolve a domain name. For more information, see “DNS Lookup Tool” on page 203.
<b>Network Status Tool</b>	Displays the server's network interface status and active connections. For more information, see “Network Status Tool” on page 220. <b>Note:</b> This tool is not supported on SiteScopes installed on UNIX platforms.
<b>Ping Tool</b>	Performs a round-trip Ping test across the network. For more information, see “Ping Tool” on page 226.
<b>Trace Route Tool</b>	Performs a traceroute from your server to another location. For more information, see “Trace Route Tool” on page 245.
<b>Operating System Tools</b>	
<b>Event Log Tool</b>	Displays portions of the Windows Event Log locally or on a remote server. For more information, see “Event Log Tool” on page 205. <b>Note:</b> This tool is not supported on SiteScopes installed on UNIX platforms.
<b>Performance Counters Tool</b>	Checks connectivity to and values in Win NT Performance Counter registries. For more information, see “Performance Counters Tool” on page 223. <b>Note:</b> This tool is not supported on SiteScopes installed on UNIX platforms.
<b>Processes Tool</b>	Shows a list of currently running processes either locally or on a remote server. For more information, see “Processes Tool” on page 228.

GUI Element	Description
<b>Services Tool</b>	Shows a list of currently running Windows Services. For more information, see “Services Tool” on page 234. <b>Note:</b> This tool is not supported on SiteScopes installed on UNIX platforms.
<b>SNMP Tools</b>	
<b>SNMP Browser Tool</b>	Browses an SNMP MIB and displays available OIDs. For more information, see “SNMP Browser Tool” on page 237.
<b>SNMP Tool</b>	Performs a SNMP get command to a specified SNMP host to retrieve a list of OIDs. For more information, see “SNMP Tool” on page 241.
<b>SNMP Trap Tool</b>	Displays the log of SNMP Traps received by SiteScope from SNMP-enabled devices. For more information, see “SNMP Trap Tool” on page 243.
<b>Web Tools</b>	
<b>FTP Server Tool</b>	Checks the availability of an FTP server and whether a file can be retrieved. For more information, see “FTP Server Tool” on page 208.
<b>URL Tool</b>	Requests a URL from a server and prints the returned data. For more information, see “URL Tool” on page 247.
<b>Web Service Tool</b>	Tests the availability of SOAP enabled Web Services. For more information, see “Web Service Tool” on page 251.

## Alerts Tab Context Menu Options

<b>Description</b>	The Context Menu Options include descriptions of the various context menu options that are available for alerts in the monitor tree and template tree.
<b>Included in Tasks</b>	“Configure an Alert” on page 1984
<b>Useful Links</b>	“SiteScope Alerts” on page 1959

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>Menu Item (A-Z)</b>	<b>Description</b>
<b>Copy</b>	Copies the alert to the selected location in the monitor tree. <b>Note:</b> Available for alerts in the <b>Alerts on Monitor/Group</b> table only.
<b>Copy to other SiteScope</b>	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Copies the alert from another SiteScope to the selected location in the monitor tree.
<b>Delete</b>	Deletes the alert.
<b>Disable Alert</b>	Disables the alert.
<b>Edit Alert</b>	Opens an editing window for the alert, which enables you to edit its settings.
<b>Enable Alert</b>	Enables the alert.
<b>New Alert</b>	Opens the New Alert dialog box, which enables you to create a new alert definition. For details on how to perform this task, see “Configure an Alert” on page 1984. <b>Note:</b> Available for alerts in the <b>Alerts on Monitor/Group</b> table only.

Menu Item (A-Z)	Description
<b>Paste</b>	Pastes the selected alert. <b>Note:</b> Available for alerts in the <b>Alerts on Monitor/Group</b> table only.
<b>Show All Descendant Alerts</b>	Displays all descendent alerts of the selected node.
<b>Show Child Alerts</b>	Displays only those alerts that are direct children of the selected node.
<b>Test</b>	Opens the Test Alert dialog box which enables you to test the alert.

## Reports Tab Context Menu Options

<b>Description</b>	The Context Menu Options include descriptions of the various context menu options that are available for Management reports in the monitor tree.
<b>Included in Tasks</b>	“Create a Report” on page 2041
<b>Useful Links</b>	“SiteScope Reports” on page 2035

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item (A-Z)	Description
<b>Clear Selection</b>	Clears the selection.
<b>Copy Report</b>	Copies the report to the selected location in the monitor tree. <b>Note:</b> Available for reports in the <b>Reports on Monitor/Group</b> table only.
<b>Create New Report</b>	Enables you to select the type of SiteScope report you want to create. For details on this topic, see “SiteScope Report Types” on page 2037. <b>Note:</b> <ul style="list-style-type: none"> <li>▶ Available for reports in the <b>Reports on Monitor/Group</b> table only.</li> <li>▶ Only Management reports are added to the Reports tab.</li> </ul>
<b>Delete Report</b>	Deletes the report.
<b>Edit Report</b>	Opens an editing window for the report, which enables you to edit its settings.
<b>Generate Report</b>	Generates the report.
<b>Paste</b>	Pastes the selected report. <b>Note:</b> Available for reports in the <b>Reports on Monitor/Group</b> table only.
<b>Select All</b>	Selects all the listed reports.
<b>Show All Descendant Reports</b>	Displays all descendent reports of the selected node.
<b>Show Child Reports</b>	Displays only those reports that are direct children of the selected node.





# 3

---

## Searching and Filtering SiteScope Objects

This chapter includes the main concepts, tasks, and reference information for searching and filtering SiteScope objects.

### **This chapter includes:**

#### Concepts

- ▶ Searching and Filtering SiteScope Objects Overview on page 105
- ▶ Defining and Managing Filter Settings on page 106
- ▶ Working with Search/Filter Tags on page 107

#### Tasks

- ▶ Create and Define a New Search/Filter Tag on page 108

#### Reference

- ▶ Search/Filter Tags User Interface on page 110

### **Searching and Filtering SiteScope Objects Overview**

When administrating monitor deployment, extensive trees displaying every object added to them could prove difficult to manage. SiteScope enables you to select which objects in the trees you want to view, based on various filter criteria. You can define multiple filters with different conditions that can be applied for varying configuration tasks.

For example, you can create a filter to display only SiteScope monitors that are monitoring CPU utilization and Disk Space. The result of this filter displays a tree with all CPU and Disk Space monitor types directly under the enterprise node.

You can also assign search/filter tags to any object in the context tree and to preference profiles, and use those tags to search or filter the display. For example, you can define a tag for all monitors running on a specific operating system.

You can also search for objects in the monitor tree by selecting a node and typing the characters you want to search in the popup search box. SiteScope begins searching as soon as you type the first character of the search string, and highlights the object with the first occurrence of the characters in the string. Click the Esc key to close the search box.

For details on filters, see “Defining and Managing Filter Settings” on page 106.

For details on tags, see “Working with Search/Filter Tags” on page 107.

## Defining and Managing Filter Settings

You define and manage views by creating and using global filters that you configure from the New/Edit Filter dialog box.

You can define filters by:

- ▶ **Monitor name.** This is done by using wild card (“\*”) and OR expressions to filter SiteScope objects appearing in the tree by the monitor name.
- ▶ **Monitor type.** For example, you can define a filter that includes all CPU monitors, regardless of their properties. In this view, the monitor tree lists all the CPU monitors defined in the SiteScope.
- ▶ **Target Server.** For example, you can define a filter that includes all SiteScope monitors with the same host defined, giving you a view of only those monitors monitoring the selected host.
- ▶ **Filter tags.** Enables you to define a filter that includes all SiteScope objects that have a specific tag value. For example, if there is a platform tag with values Windows, Linux, AIX, and Solaris, you can filter for all objects that have the AIX tag value assigned to them.

- ▶ **Monitor status (enabled/disabled).** Enables you to define a filter that includes only enabled or disabled SiteScope monitors.
- ▶ **HP Business Availability Center logging.** Enables you to define a filter that includes monitors based on their settings for reporting data to Business Availability Center.

---

**Note:** To create a filter based on specific common properties, use Global Search and Replace. For details, see “Global Search and Replace” on page 171.

---

If you have any filters defined, they appear in the drop-down filter list above the monitor tree. You select the filter from the list and the tree displays only those objects defined in your filter selection.

## Working with Search/Filter Tags

You create custom search/filter tags for use in filtering the display of the left tree pane for SiteScope objects (groups, monitors, templates, and preference profiles). You define the tags and their values, and assign these to the different elements in your enterprise.

For example, you define a tag called Priority with the possible values of Critical, High, Medium, and Low. You assign these tag values to different elements in the infrastructure. Monitors of Web servers and databases that support 24x7 customer access could be assigned a category value of Priority: Critical. While adding a new filter setting, you select **Tags** in the Filter Options section, enter Priority:Critical as the value of the object, and click **Save**. This filter displays only those elements to which you assigned this tag and value.

## **Create and Define a New Search/Filter Tag**

This task describes the steps involved in defining a new search/filter tag and assigning it to one or more elements in the context tree.

This task includes the following steps:

- ▶ “Create a Search/Filter Tag” on page 108
- ▶ “Assign Search/Filter Tags to SiteScope Tree Elements” on page 108
- ▶ “Define a Tag for a Filter Setting” on page 109

### **1 Create a Search/Filter Tag**

You use the **Search/Filter Tags** panel of the SiteScope object to add search/filter tags.

For details on the user interface, see “Search/Filter Tags” on page 375.

For details on adding a tag, see “New/Edit Tag Dialog Box” on page 116.

### **2 Assign Search/Filter Tags to SiteScope Tree Elements**

Before you can use a tag as part of a view filter, you must assign it to one or more elements in the context tree or to preference profiles. You can assign tags to any item in the tree, including any container, monitor, group, or alert.

You assign tags while adding, importing, or editing context tree objects or preference profiles. Tags are included as properties for every type of object in the context tree.

For details on the objects in the monitor tree, see “Monitor Tree” on page 72.

For details on the objects in the template tree, see “Template Tree” on page 84.

### 3 Define a Tag for a Filter Setting

Once you have assigned the tag to one or more items in the context tree or preference profiles, you can use the tag as an object for a filter.

For details on filtering in the user interface, see “New/Edit Filter Dialog Box” on page 111.

#### Example

Create a tag indicating the type of operating system on which the monitors are running. The tag Operating Systems would have values such as Windows 2000, Windows XP, Solaris, Linux, and so forth.

Enter a name and description for the tag, and add tag values. The tag will be added to the list of tags in [Search/Filter Tags](#) Preferences.

Tag name: \*

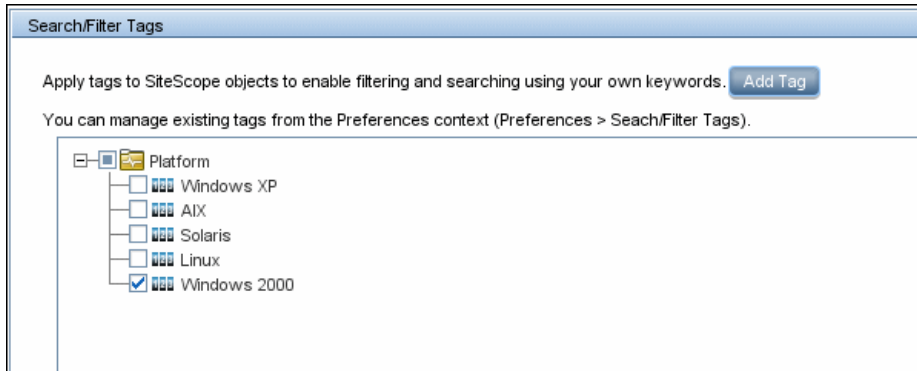
Tag description:

Values:

Value Name	Value Description
Windows 2000	
Windows XP	
Linux	
Solaris	
AIX	

OK Cancel Help

Assign the tag to a monitor tree element such as a group, by opening the Search/Filter Settings for the group, and selecting Windows 2000 as the value under the Operating Systems tag.





Using this new tag, you could define a filter setting for the monitor tree to display only those monitors running on Windows machines.

## Search/Filter Tags User Interface

**This section includes (in alphabetical order):**


- New/Edit Filter Dialog Box on page 111
- New/Edit Tag Dialog Box on page 116

## New/Edit Filter Dialog Box



<b>Description</b>	<p>Enables you to add a new filter or edit an existing one when working in the monitor tree.</p> <p><b>To access:</b> In the context toolbar (above the left tree pane), click the arrow next to the <b>Filter</b>  button, and select <b>New Filter</b>, or select an existing filter and click <b>Edit</b>. After a filter has been applied, the filter icon is displayed as .</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Searching and Filtering SiteScope Objects Overview” on page 105</li> <li>➤ “Defining and Managing Filter Settings” on page 106</li> <li>➤ “Tree Toolbar Buttons” on page 65</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):



GUI Element	Description
<b>General Settings</b>	
<b>Filter name</b>	Enter a filter name. This name appears in the list of available filters when you click the <b>Filter</b> arrow.
<b>Filter description</b>	<p>You can enter a description for the filter. This description appears only when editing the filter.</p> <p><b>Note:</b> This field is optional.</p>
<b>Public</b>	<p>Describes the permissions of the filter. If the filter is public, all users can see, use, and edit the filter, but only the public filter owner can change this filter to a private filter.</p> <p>If the filter is not public, only the current user can see and use it.</p>

GUI Element	Description
<b>Filter Options</b>	
<b>Monitor name</b>	<p>To filter the objects appearing in the tree by the monitor name, type a monitor name.</p> <ul style="list-style-type: none"> <li>▶ The monitor name is the string entered in the <b>Name</b> box in the General Settings area during monitor configuration.</li> <li>▶ Enter a regular expression to widen the filter. You can use the wild card character ("*") and <b>or</b> expressions.</li> </ul> <p>The monitor tree displays only those monitors, within their groups, matching the string entered and only those groups containing these monitors.</p> <p><b>Example:</b> The expression /URL Monitor.* \.gov/ matches all monitor names containing the string URL Monitor with addresses containing the domain .gov.</p> <p><b>Note:</b> This field is case sensitive.</p>
<b>Monitor type</b>	<p>To filter the objects appearing in the tree by the monitor type, enter the monitor type, or click the <b>Browse</b>  button and select the monitor types by which you want to filter in the Monitors list.</p> <p>For details on the Filter Monitor Types user interface, see “Filter Monitor Types Dialog Box” on page 114.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ When entering multiple monitors, separate them with a comma (",").</li> <li>▶ When entering a monitor type, you can use the wild card character ("*") and <b>or</b> expressions.</li> </ul> <p><b>Example:</b> SAP* or CPU*</p>



GUI Element	Description
<b>Target server</b>	<p>To filter the objects appearing in the tree by the target server, type a server name or click the <b>Browse</b>  button and select the remote servers by which you want to filter from the Targets list.</p> <ul style="list-style-type: none"> <li>▶ The target is the string entered in the <b>Server</b> box in the Monitor Settings area during monitor configuration.</li> <li>▶ Enter a regular expression to widen the filter. You can use the wild card character ("*") and <b>or</b> expressions.</li> </ul> <p>The tree displays only those monitors, within their groups, whose target server matches the string entered and only those groups containing these monitors.</p> <p>For details on the Filter Targets user interface, see “Filter Target Servers Dialog Box” on page 115.</p> <p><b>Note:</b> When entering multiple targets, separate them with a comma (",").</p>
<b>Tags</b>	<p>Enter tag values, or click the <b>Browse</b>  button and select the tag values by which you want to filter in the Tags list. For details on the Filter Tags user interface, see “Filter Tags Dialog Box” on page 116.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ When entering multiple tag values, separate them with a comma (",").</li> <li>▶ You can use the wild card character ("*") and <b>or</b> expressions to filter tag values.</li> </ul>
<b>Enable/Disable monitor</b>	<p>Select the monitor status (enabled/disabled) by which you want to filter.</p> <p><b>Default value:</b> None</p>
<b>HP BAC Logging</b>	<p>Select a BAC logging option by which to filter.</p> <p>For details on the logging options, see “HP BAC Integration Settings” on page 370.</p>



## Filter Monitor Types Dialog Box

<b>Description</b>	<p>Enables you to select the monitor type by which you can filter SiteScope objects.</p> <p><b>To access:</b> In the context toolbar, click the arrow next to the <b>Filter</b>  button, and select <b>New Filter</b>, or select an existing filter and click <b>Edit</b>. In the New/Edit Filter dialog box, click the <b>Browse</b>  button next to <b>Monitor Type</b>.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Searching and Filtering SiteScope Objects Overview” on page 105</li> <li>▶ “Defining and Managing Filter Settings” on page 106</li> <li>▶ “New/Edit Filter Dialog Box” on page 111</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Available Monitor Types</b>	<p>Displays the available monitor types.</p> <p>Select the monitor types you want to include in the filter and click the <b>Move to Selected Monitor Types list</b> button. The selected monitor types are moved to the Selected Monitor Types list.</p>
<b>Selected Monitor Types</b>	<p>Displays the monitor types currently selected for this filter.</p> <p>To remove monitor types from this list, select the monitor types and click the <b>Remove from Selected Monitor Types list</b> button. The measurements are moved to the Available Monitor Types list.</p>



## Filter Target Servers Dialog Box

<b>Description</b>	<p>Enables you to filter SiteScope objects by the selected server targets configured in SiteScope.</p> <p><b>To access:</b> In the context toolbar, click the arrow next to the <b>Filter</b>  button, and select <b>New Filter</b>, or select an existing filter and click <b>Edit</b>. In the New/Edit Filter dialog box, click the <b>Browse</b>  button next to <b>Target Server</b>.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Searching and Filtering SiteScope Objects Overview” on page 105</li> <li>▶ “Defining and Managing Filter Settings” on page 106</li> <li>▶ “New/Edit Filter Dialog Box” on page 111</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Available Target Servers</b>	<p>Displays the remote servers available in SiteScope.</p> <p>Select the remote servers you want to include in the filter and click the <b>Move to Selected Target Servers list</b> button. The selected remote servers are moved to the Selected Target Servers list.</p>
<b>Selected Target Servers</b>	<p>Displays the remote servers currently selected for this filter.</p> <p>To remove remote servers from this list, select the remote servers and click the <b>Remove from Selected Target Servers list</b> button. The measurements are moved to the Available Target Servers list.</p>

## Filter Tags Dialog Box

<b>Description</b>	<p>Enables you to select the tag values by which you can filter SiteScope objects.</p> <p><b>To access:</b> In the context toolbar, click the arrow next to the <b>Filter</b>  button, and select <b>New Filter</b>, or select an existing filter and click <b>Edit</b>. In the New/Edit Filter dialog box, click the <b>Browse</b>  button next to <b>Tags</b>.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Searching and Filtering SiteScope Objects Overview” on page 105</li> <li>▶ “Defining and Managing Filter Settings” on page 106</li> <li>▶ “New/Edit Filter Dialog Box” on page 111</li> </ul>





The following elements are included (unlabeled GUI elements are shown in

GUI Element	Description
<Tag name and values>	<p>Displays the tag names and tag values if tags have been created. Select the check box next to the tags that you want to include in the filter, and click <b>Save</b>.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>

## New/Edit Tag Dialog Box

<b>Description</b>	<p>Enables you to add a new search/filter tag.</p> <p><b>To access:</b> Select a SiteScope object (group, monitor, template, or preference profile), and open the <b>Search/Filter Tags</b> panel in the Properties tab or preference profile page. Click the <b>Add Tag</b> button.</p>
<b>Important Information</b>	<p>You can edit existing tags in the Preferences context (<b>Preferences &gt; Search/Filter Tags</b>). For details on this topic, see “Search/Filter Tags Overview” on page 1533.</p>
<b>Included in Tasks</b>	<p>“Create and Define a New Search/Filter Tag” on page 108</p>
<b>Useful Links</b>	<p>“Working with Search/Filter Tags” on page 107</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click the <b>New</b> button to add a tag value. A new row is added at the bottom of the list of tag values.
	Click the <b>Delete</b> button to delete the selected value from the tag.
	Click the <b>Move up tag value</b> button to move up the list of tag values from the selected value.
	Click the <b>Move down tag value</b> button to move down the list of tag values from the selected value.
<b>Tag name</b>	The name of the search/filter tag. <b>Maximum length:</b> 255 characters
<b>Tag description</b>	A description of the search/filter tag.
<b>Values</b>	The values included in the tag.
<b>Value Name</b>	Enter a name for the value to be included in the tag. Each tag must include at least one value. Each value appears as a child object of the tag name when defining or editing tag settings for all objects in the monitor tree.
<b>Value Description</b>	Enter an optional description for each value. This description appears only when editing the tag.



# 4

---

## System Availability Management Administration

This chapter includes the main concepts, tasks, and reference information for System Availability Management Administration.

**This chapter includes:**

**Concepts**

- ▶ System Availability Management Administration Overview on page 120

**Tasks**

- ▶ Manage Multiple SiteScopes in System Availability Management on page 121

**Reference**

- ▶ System Availability Management Administration User Interface on page 124
- ▶ **Troubleshooting and Limitations** on page 146

## **System Availability Management Administration Overview**

You install SiteScope on designated host machines with access to the applications and operating systems to be monitored. SiteScope collects key performance measurements on a wide range of back- and front-end infrastructure components, including Web, application, database, and firewall servers.

SiteScope can be accessed as a standalone application or using System Availability Management Administration from within HP Business Availability Center or HP Operations Manager. (Windows-based and Solaris-based SiteScope installations both work with Windows-based or Solaris-based HP Business Availability Center servers.)

System Availability Management Administration enables you to register, configure and maintain your SiteScope servers. You can configure and manage multiple SiteScopes from within System Availability Management Administration. You can configure SiteScope monitors, alerts, and reports and make any other configuration changes for the SiteScope. All the configuration changes that are done from System Availability Management Administration are reflected in the SiteScope itself.

System Availability Management enables you to:

- ▶ Add SiteScopes to System Availability Management Administration. For details on the user interface, see “New SiteScope Page” on page 133.
- ▶ Copy group, monitor, report, and alert instances from one SiteScope to another SiteScope using copy/paste. For details on this topic, see “Copying and Moving SiteScope Objects” on page 61.
- ▶ Synchronize a SiteScope’s settings with another SiteScope by copying settings, preferences, and template files using the Sync SiteScope wizard. For details on the user interface, see “Sync SiteScopes Wizard - Select Source and Targets Page” on page 139.
- ▶ Perform a Global Replace operation across multiple SiteScopes. For details, see “Global Search and Replace Wizard” on page 178.



- View accessibility information and summary information regarding registration status of the SiteScope to Business Availability Center, licence points, sample reporting rates, monitor run rates and health of the SiteScopes. For details on the user interface, see “System Availability Management Administration” on page 125.
- Run the Monitor Deployment Wizard to deploy monitors onto configuration items in Business Availability Center’s CMDB. (This feature is not available to users accessing SiteScope from HP Operations Manager.) For details on the user interface, see “Monitor Deployment Wizard” on page 1811.

## **Manage Multiple SiteScopes in System Availability Management**

This task describes how to work with System Availability Management to manage multiple SiteScopes.

This task includes the following steps:

- “Prerequisites” on page 122
- “Add a SiteScope to System Availability Management Administration” on page 122
- “Configure Integration Preferences” on page 122
- “Use the Sync SiteScopes Wizard to Update Properties - Optional” on page 123
- “Perform a Global Search and Replace - Optional” on page 123
- “Copy Monitoring Objects from One SiteScope to Another SiteScope - Optional” on page 123
- “View Accessibility, License, and Monitoring Data for All Registered SiteScopes” on page 124

## 1 Prerequisites

You must have at least one SiteScope running in a network location that is accessible to the System Availability Management application.

If you are working in HP Business Availability Center, you can download SiteScope from the Downloads page in Platform Administration.

## 2 Add a SiteScope to System Availability Management Administration

Add one or more SiteScope profiles. While entering the information in the New SiteScope page, keep the following in mind:

The following fields are mandatory:

- ▶ **Display Name.** Enter a name to represent this SiteScope in Business Availability Center and HP Operations Manager applications and in System Availability Management Administration.
- ▶ **Host Name.** If you are using a Business Availability Center with Lightweight Single Sign-on enabled (by default), you must enter a fully qualified domain name as the host name.
- ▶ **Port Number.** The default value is **8080**. If the port number used to communicate with SiteScope is different than 8080, enter it here.

For details on the user interface, see “New SiteScope Page” on page 133.

## 3 Configure Integration Preferences

Access the Integration Preferences within the SiteScope interface and modify the fields as necessary.

For details on how to perform this task, see “Configure SiteScope-HP Business Availability Center Integration Preferences for Inaccessible Profiles” on page 1423.

For details on this concept, see “Integration Preferences Overview” on page 1416.

For details on the user interface, see “Integration Preferences User Interface” on page 1429.

## 4 Use the Sync SiteScopes Wizard to Update Properties - Optional

You can use the Sync SiteScopes wizard to update the properties of all the SiteScopes in System Availability Management Administration. This is useful for copying configuration objects, such as templates, alert templates, schedule preferences, MIB files, and script files, from one SiteScope to one or multiple SiteScopes in your network environment.

For details on the user interface, see “Sync SiteScopes Wizard - Select Source and Targets Page” on page 139.

## 5 Perform a Global Search and Replace - Optional

Use the Global Search and Replace Wizard to replace values across multiple SiteScopes. This is useful for when you must update values pertaining to the integration between SiteScope and Business Availability Center or for enterprise level updates to perform across multiple SiteScopes and large monitoring environments.

For details on how to perform this task, see “Perform a Global Search and Replace” on page 174.

## 6 Copy Monitoring Objects from One SiteScope to Another SiteScope - Optional

Once you have multiple SiteScopes running in System Availability Management Administration, you can copy monitoring and other SiteScope objects from one SiteScope to another. You can copy multiple or single groups, monitors, and alerts.

Right-click the object to be copied and select **Copy** from the context menu. Highlight the parent object to where you want to copy, right-click and select **Paste** from the context menu. The source and the target can be in different SiteScopes.

---

**Note:** When copying monitors, groups, or other entities between multiple SiteScope instances, tag assignments are lost even if the tags that were assigned to the copied entities on the source SiteScope are present on the target SiteScope.

---

## 7 View Accessibility, License, and Monitoring Data for All Registered SiteScopes

The main page of System Availability Management Administration enables you to view the details of your multiple SiteScopes.

For details on the user interface, see “System Availability Management Administration” on page 125.

## System Availability Management Administration User Interface

### **This section includes:**

- ▶ System Availability Management Administration on page 125
- ▶ New SiteScope Page on page 133
- ▶ Sync SiteScopes Wizard - Select Source and Targets Page on page 139

---

**Note:** System Availability Management Administration is available only to those users accessing SiteScope from HP Business Availability Center.




---





## System Availability Management Administration

<p><b>Description</b></p>	<p>System Availability Management Administration is a portal within HP Business Availability Center that enables you to add SiteScope servers to an HP Business Availability Center system and to access those SiteScope servers.</p> <p>The SiteScopes are represented as nodes in the tree in the left pane.</p> <ul style="list-style-type: none"> <li>▶ When you highlight the root node, the right pane displays the System Availability Management functions, including summary information for the SiteScopes.</li> <li>▶ When you highlight a SiteScope in the tree, the right pane displays that SiteScope's Dashboard and you can perform any function within the SiteScope.</li> </ul> <p><b>To access:</b> Select <b>Admin &gt; System Availability Management</b>.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Each SiteScope is listed by name with an icon displaying its current connection status to HP Business Availability Center.</li> <li>▶ You access the SiteScope server by highlighting the name of the server in the list in the left pane.</li> <li>▶ If a SiteScope is restarted while being accessed in System Availability Management Administration, you may receive an error and have to renavigate to the SiteScope to properly access the SiteScope server.</li> </ul>

## List of SiteScope Servers - Left Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<SiteScope server name>	<p>Represents an individual SiteScope server.</p> <p>The name includes a tooltip that displays the following data:</p> <ul style="list-style-type: none"> <li>▶ <b>Health.</b> Health status of the SiteScope server represented by a status icon.</li> <li>▶ <b>Mode.</b> Whether the SiteScope is currently hosted by the HP Business Availability Center.</li> <li>▶ <b>Points.</b> The number of license points in use by the SiteScope.</li> <li>▶ <b>Remote server.</b> The number of remote servers being monitored by this SiteScope.</li> <li>▶ <b>Operating system.</b> The type of operating system on which the SiteScope is running.</li> <li>▶ <b>High Availability server.</b> The name of the server used by this SiteScope for failover.</li> </ul>
	<p>Icon accompanying the SiteScope name indicating that the SiteScope is registered to HP Business Availability Center and fully accessible from System Availability Management Administration. A SiteScope with this status is considered 'hosted' by HP Business Availability Center.</p>
	<p>Icon accompanying the SiteScope name indicating that the SiteScope is registered to HP Business Availability Center but not available for configuring. A SiteScope with this status reports data to HP Business Availability Center but can be configured only when accessing the SiteScope standalone.</p>
	<p>Icon accompanying the SiteScope name indicating that the existing SiteScope profile is empty and there is no running SiteScope associated with it.</p>

GUI Element	Description
	Icon accompanying the SiteScope name indicating that the integration between HP Business Availability Center and the SiteScope has been reset. The profile remains in HP Business Availability Center and can be used to prepare history reports. Data, however, is not reported to HP Business Availability Center applications.
	Click to add a SiteScope. Opens the New SiteScope page.
	Click to edit the properties of the highlighted SiteScope's connection to this HP Business Availability Center. Opens the Edit SiteScope page.
	Click to delete the highlighted SiteScope from this HP Business Availability Center.

### Context Menu Options

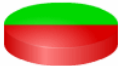

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Menu Item	Description
<b>New SiteScope</b>	When highlighting the root node, click to add a SiteScope to the list of SiteScopes that are accessible to this HP Business Availability Center. Opens the New SiteScope page.
<b>Edit SiteScope</b>	Click to edit the properties of the highlighted SiteScope's connection to this HP Business Availability Center. Opens the Edit SiteScope page.
<b>Delete SiteScope</b>	Click to delete the highlighted SiteScope from this HP Business Availability Center.

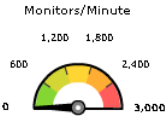
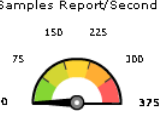


## Summary Information - Right Pane

<p><b>Description</b></p>	<p>When you highlight the root node, the right pane displays the summary information for all the SiteScopes accessed by this HP Business Availability Center.</p> <p><b>To access:</b> Select <b>Admin &gt; System Availability Management</b> and highlight the root node in the left pane.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ You access the SiteScope server by highlighting the name of the server in the list in the left pane or by clicking the name of the SiteScope in the table.</li> <li>▶ The graphs displayed at the top of the page are a summary of all the SiteScopes listed.</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<p>Health</p> 	<p>Graph represents the overall health status of the listed SiteScopes. Each SiteScope represents its proportionate section of all the SiteScopes attached to HP Business Availability Center.</p>
<p>Points Used/Total</p> 	<p>Gauge represents the current monitor points that are in use by all the registered and configurable (hosted) SiteScopes versus the total points available for this installation.</p> <p><b>Note:</b> The points displayed are per individual SiteScope. You cannot share license points among SiteScopes but you can shift a license key from one SiteScope to another. Delete the license key from the SiteScope that no longer uses that license and enter the same license key in the SiteScope that you want to use the license. For details on entering license information, see “General Preferences User Interface” on page 1379.</p>







GUI Element	Description
 <p>Monitors/Minute 0 600 1,200 1,800 2,400 3,000</p>	<p>Gauge represents the total runs per minute and is calculated by taking the sum of all monitor runs per minute for all the hosted SiteScopes versus the number of hosted SiteScopes times 1000 (the maximum number of monitor runs per minute).</p>
 <p>Samples Report/Second 0 75 150 225 300 375</p>	<p>Gauge displaying the rate of samples being reported from all SiteScopes to HP Business Availability Center. The maximum number of samples per second is determined by the HP Business Availability Center deployment.</p>
	<p>You can adjust the width of the table's columns by dragging the borders of the column to the right or the left.</p> <p>Click to reset the table columns' width to their default setting.</p>
	<p>Click to open the Select Columns dialog box and select the columns you want displayed in the table.</p>
<p><b>Global Search and Replace</b></p>	<p>Click to open the Global Search and Replace Wizard to update properties across multiple SiteScopes. For details on the user interface, see “Global Search and Replace Wizard” on page 178.</p>
<p><b>Sync SiteScopes</b></p>	<p>Click to open the Sync SiteScope Wizard to copy preferences, settings, and configuration files between SiteScopes. For details on the user interface, see “Sync SiteScopes Wizard - Select Source and Targets Page” on page 139.</p>

### SiteScope Summary Table

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Table Column	Description
<b>Display Name</b>	The name give to the SiteScope when it was added to System Availability Management Admin.
<b>Points Used/Total</b>	The number of license points currently being used by the SiteScope versus the total license points available.
<b>Deployed Monitors</b>	The number of monitors configured the specific SiteScope server.
<b>Monitors/Minute</b>	The number of monitor runs per minutes.
<b>Remote Targets</b>	Displays the number of remote servers being monitored by this SiteScope.
<b>OS</b>	The operating system on which the SiteScope is running.
<b>Version</b>	The version of the SiteScope software.
<b>Samples/Report</b>	Displays the rate of samples reported from this SiteScope to HP Business Availability Center.
<b>HA Status</b>	Displays whether the failover SiteScope installation is running or not and whether the failover SiteScope is running instead of the primary SiteScope.

Table Column	Description
<p><b>Health</b></p>	<p>Indicates the status of the SiteScope itself. The following are the available status levels:</p> <ul style="list-style-type: none"> <li> <b>OK.</b> All performance measurements are within the OK threshold level.</li> <li> <b>Warning.</b> At least one performance measurement is within the Warning range, but no measurements are within the Error or Poor range.</li> <li> <b>Error/Poor.</b> At least one performance measurement is within the Error or Poor range. This indicates either of the following: <ul style="list-style-type: none"> <li>▶ the performance measurement has a value, but at poor quality level</li> <li>▶ there is no measurement value due to some error</li> </ul> </li> <li> <b>No thresholds breached.</b> No thresholds were defined for the monitor, so no status is assigned.</li> </ul>
<p><b>SAM Points Used</b></p>	<p>Displays the number of points used by monitors currently enabled and reporting to HP Business Availability Center from this SiteScope.</p> <p><b>Note:</b> These points do not include Technology Integration Monitor points.</p> <p>This number differs from the <b>Points Used/Total</b> field which is the number of points currently in use versus the total number of points available for the SiteScope.</p>
<p><b>MDW</b></p>	<p>Click to access the Monitor Deployment Wizard. You use the wizard to deploy monitors from the SiteScope onto existing CIs in HP Business Availability Center.</p>

## Optional Columns for SiteScope Summary Table

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Table Column	Description
<b>Last Report Time</b>	The last time monitor data was reported to Business Availability Center, displayed in format: Day Month Date Hours:Minutes:Seconds.
<b>Host Name</b>	The host name or IP address of the machine on which the SiteScope is currently running.
<b>Port Number</b>	The port number used to communicate with SiteScope. <b>Default value:</b> 8080
<b>Inaccessible Profile</b>	Displays if this SiteScope profile was added to System Availability Management Administration without a running SiteScope server registered to it. This means that the profile name was added to the database but there is no connection to the SiteScope from HP Business Availability Center until the actual registration from the SiteScope server.
<b>Use SSL</b>	Displays whether this SiteScope is using a secure communication through HTTPS.
<b>Profile Name</b>	The name to identify this SiteScope for HP Business Availability Center operations and reports. <b>Note:</b> If no value is entered, the <b>Display Name</b> entered in the Main Settings is used.
<b>GMT Offset</b>	The GMT Offset set for the SiteScope profile used for reports and aggregation purposes.
<b>Enable Reporting to HP BAC</b>	Displays whether the SiteScope is enabled to forward measurements to HP Business Availability Center.
<b>GW Server Name</b>	The name or IP address of HP Business Availability Center's Gateway server.

Table Column	Description
Failover Host	Displays the host name of the failover server if one has been installed for this SiteScope.
Description	The description of this SiteScope as entered when adding the SiteScope to System Availability Management Administration.

## New SiteScope Page

Description	Use to add an existing SiteScope to this HP Business Availability Center. You can determine whether the SiteScope is hosted by System Availability Management or if it just reports data to HP Business Availability Center.
Important Information	<ul style="list-style-type: none"> <li>▶ Once a SiteScope is added to the System Availability Management page, it is assigned a connectivity status.</li> <li>▶ Only a user who is defined with Administrator permissions in SiteScope standalone can add that SiteScope to System Availability Management Administration.</li> </ul>
Useful Links	“System Availability Management Administration” on page 125

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Display Name</b>	Enter a descriptive name representing this SiteScope in System Availability Management Admin. This name identifies the SiteScope in the list of SiteScopes in the left pane and in the summary list in the right pane.
<b>Host Name</b>	Enter the host name or IP address of the machine on which SiteScope is currently running. <b>Note:</b> If the Business Availability Center you are using uses Lightweight Single Sign-on (enabled by default), you must enter a fully qualified domain name. <b>Example:</b> lab1.emea.hp
<b>Port Number</b>	Enter the port number used to communicate with SiteScope. <b>Default value:</b> 8080
<b>Inaccessible Profile</b>	Use this box to create a profile for a SiteScope that is not currently accessible from HP Business Availability Center. Creating the profile in this way adds the profile name to the database but there is no connection to the SiteScope from HP Business Availability Center until the actual registration from the SiteScope. Registering a SiteScope to an empty profile is done in SiteScope by creating an integration setting for BAC in <b>Preferences &gt; Integration Preferences</b> . <b>Example:</b> Enter a profile name for a SiteScope to report data to HP Software-as-a-Service. HP Software-as-a-Service cannot access the SiteScope until it has been registered from the SiteScope.

## Distributed Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Gateway Server name/IP address</b>	By default, this box displays the name or IP address of the Gateway server.  <b>Note:</b> Modify this box only if the HP Business Availability Center has a distributed deployment and the Gateway server is installed on different machines. In this case, enter the name or IP address of the Core server.
<b>SiteScope agent machine location</b>	Enter the SiteScope agent machine location. If no value is entered, the default is used.
<b>Gateway Server authentication user name</b>	Enter the login user name used to access the Gateway server. If no value is entered, the default is used.
<b>Gateway Server authentication password</b>	Enter the password used to access the Gateway server. If no value is entered, the default is used.

## Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>SiteScope user name</b>	Enter the user name needed to connect to the SiteScope.
<b>SiteScope password</b>	Enter the SiteScope login password if the SiteScope you are adding has been set up with a password.
<b>Failover Host</b>	If a failover server has been installed for this SiteScope, enter the host name.  <b>Note:</b> There is no validation to check if there is a failover SiteScope running on this host.
<b>Description</b>	Enter a description for this SiteScope.

## Profile Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Use SSL</b>	Select to secure the communication of the SiteScope API through a secure HTTPS. Selecting this option requires you to configure your SiteScope to run with SSL.
<b>Profile name</b>	Enter a name to identify this SiteScope for HP Business Availability Center operations and reports. If no value is entered, the <b>Display Name</b> entered in the Main Settings is used.
<b>GMT offset</b>	Select the GMT Offset for the SiteScope profile used for reports and aggregation purposes.
<b>Profile database name</b>	Select the database (Microsoft SQL) or schema (Oracle) into which the profile information is saved.
<b>Web server authentication user name</b>	Enter the user name for the authentication (basic authentication and protocol) of the Web server security options.
<b>Web server authentication password</b>	Enter the password for the authentication of the Web server security options (basic authentication and protocol).
<b>Web server use SSL</b>	Select this option for the Web server to use https protocol over a secure connection.
<b>Proxy name/IP address</b>	If SiteScope uses a proxy to connect to the HP Business Availability Center server, enter the IP address.
<b>Proxy user name</b>	If SiteScope uses a proxy to connect to the HP Business Availability Center server, enter the user name for the proxy.



GUI Element	Description
<b>Proxy password</b>	If SiteScope uses a proxy to connect to the HP Business Availability Center server, enter the password for the proxy.
<b>Enable Reporting to BAC</b>	Enables reporting SiteScope measurements to HP Business Availability Center. You can clear this option to temporarily disable reporting from this SiteScope to HP Business Availability Center. <b>Default value:</b> Selected. Can be cleared only in edit mode and not when adding a SiteScope.

### Topology Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Topology resynchronization time interval</b>	The number of days for SiteScope to synchronize topology data with Business Availability Center. The topology information SiteScope reports to Business Availability Center is synchronized when SiteScope restarts after this time interval has been reached. SiteScope restarts by default every 24 hours. <b>Default value:</b> 7 (days) <b>Note:</b> All topologies created by SiteScope and stored in CMDB are subjected to the aging process. To prevent aging, see “Aging of CIs in CMDB” on page 158.
<b>Default topology probe domain</b>	Enter the default domain of the SiteScope topology probe. <b>Note:</b> You must restart SiteScope if you change this setting.

GUI Element	Description
<b>Topology receiver port</b>	Enter the topology receiver port used in Business Availability Center. <b>Default value:</b> 8080 <b>Note:</b> You must restart SiteScope if you change this setting.
<b>Topology receiver SSL port</b>	Enter the topology receiver SSL port used in Business Availability Center. <b>Default value:</b> 443 <b>Note:</b> You must restart SiteScope if you change this setting.

---

**Note:** The following settings can only be modified in the user interface, and not from the `<SiteScope root directory>\conf\ems\jython.properties` file:

- **Default topology probe domain** (appilog.collectors.domain)
- **Topology receiver port** (serverPort)
- **Topology receiver SSL port** (serverPortHttps)

If you modified these settings from the properties file in a previous version of SiteScope (the property name is shown in brackets), these changes are lost when upgrading to SiteScope 9.50 and you must reconfigure the settings in the user interface. If you modified the remaining settings, these changes are lost when upgrading to SiteScope 9.50, and you must reconfigure the settings in the

`<SiteScope root directory>\discovery\discovery_agent.properties` file.

---

## Sync SiteScopes Wizard - Select Source and Targets Page

<p><b>Description</b></p>	<p>Use this wizard to synchronize settings from different SiteScopes by copying files and settings from one SiteScope to another.</p> <p><b>To Access:</b></p> <p>Select <b>Admin &gt; System Availability Management</b> and click <b>Sync SiteScopes</b>.</p> <p>Use the Select Source and Targets page to select the source SiteScope from which to copy settings and the target SiteScope to which to copy settings.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This wizard can be used to copy the settings configured for a SiteScope to another SiteScope.</li> <li>▶ To copy groups, monitors, alerts, or reports from one SiteScope to another SiteScope, use the <b>Copy</b> and <b>Paste to another SiteScope</b> option in the monitor tree's context menu.</li> <li>▶ The Select Source and Targets page lists only those SiteScopes that:             <ul style="list-style-type: none"> <li>▶ are version 9.0 or higher</li> <li>▶ have been added to System Availability Management</li> <li>▶ are currently accessible to HP Business Availability Center</li> </ul> </li> </ul>
<p><b>Wizard Map</b></p>	<p>The Sync SiteScopes wizard includes: <b>Sync SiteScopes Wizard - Select Source and Targets Page</b> &gt; Select Types to Sync &gt; Select Instances to Sync &gt; Summary Page.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Source SiteScope</b>	<p>Select the SiteScope from which to copy settings or files. You can select only one SiteScope from which to copy.</p> <p>Once a SiteScope is selected as the source, it cannot be selected as a target.</p> <p><b>Note:</b> Only those SiteScopes appear for which the current user has at least view permissions as applied in Permissions Management. For details on this topic, see “Operations” in <i>Platform Administration</i> in the HP Business Availability Center Documentation Library.</p>
<b>Target SiteScope</b>	<p>Select the SiteScopes to which to copy settings or files. You can select multiple SiteScopes as the target of the synchronization.</p> <p><b>Note:</b> Only those SiteScopes appear for which the current user has at least change permissions as applied in Permissions Management. For details on this topic, see “Operations” in <i>Platform Administration</i> in the HP Business Availability Center Documentation Library.</p>

### **Select Types to Sync**

<b>Description</b>	<p>Use this page to select those objects, settings, or files to copy from one SiteScope to other SiteScopes.</p> <p>You can copy preferences, views, and categories. Only those objects appear that have been configured in the source SiteScope.</p>
<b>Important Information</b>	<p>You can use the <b>Select All</b>, <b>Clear Selection</b>, and <b>Invert Selection</b> buttons to modify your selections.</p>
<b>Wizard Map</b>	<p>The Sync SiteScopes wizard includes: Sync SiteScopes Wizard - Select Source and Targets Page &gt; <b>Select Types to Sync</b> &gt; Select Instances to Sync &gt; Summary Page.</p>

## SiteScope Objects

The following are the objects that can be copied from one SiteScope to other SiteScopes:

GUI Element	Description
<p><b>Preferences</b></p>	<p>Copy the preferences configured in the source SiteScope to the target SiteScope. Only those preferences that have been configured in the source SiteScope appear here. If no preferences or instances of preference types have been defined in the source SiteScope, there are no preferences listed here.</p> <p>The following preferences can be selected for the sync operation:</p> <ul style="list-style-type: none"> <li>➤ Email preferences</li> <li>➤ Pager preferences</li> <li>➤ SNMP trap preferences</li> <li>➤ Absolute schedule preferences</li> <li>➤ Range schedule preferences</li> </ul> <p>For details on types of preferences, see “Preferences Menu” on page 93.</p> <p><b>Example:</b> Copy the absolute schedules that have been configured in the source SiteScope to the target SiteScope. You can then use those same absolute schedules when scheduling monitors to run (while configuring or editing monitors) in the target SiteScope.</p>

GUI Element	Description
<b>Categories (Search/Filter tags in SiteScope 10.00)</b>	<p>Copy the categories configured in the source SiteScope to the target SiteScope. If no categories have been defined in the source SiteScope, there are no categories listed here. In SiteScope 10.00 and later, categories are known as Search/Filter tags and include the same functionality.</p> <p>For details about using categories (Search/Filter tags) in SiteScope, see “Working with Search/Filter Tags” on page 107.</p> <p><b>Example:</b> A category defining operating system with values of Windows, Linux, and so forth has been defined in the source SiteScope. These same categories can be copied for use in the target SiteScope.</p>
<b>Templates</b>	<p>Copy the templates configured in the source SiteScope to the target SiteScope. If no templates have been defined in the source SiteScope, there are no templates listed here.</p> <p>For details about working with templates in SiteScope, see “SiteScope Templates Overview” on page 1558.</p>

### SiteScope Files

The following are the files that can be copied from one SiteScope to other SiteScopes:

GUI Element	Description
<b>SNMP Template Files</b>	<p>Templates that can be selected when creating an SNMP trap alert action.</p> <p>Select to copy all the files in the following folder path:  <b>&lt;SiteScope root directory&gt;\templates.snmp.</b></p>
<b>Certificate Template Files</b>	<p>Select to copy all the files in the following folder path:  <b>&lt;SiteScope root directory&gt;\templates.certificates.</b></p>
<b>Post Template Files</b>	<p>Templates that can be selected when creating a post alert action.</p> <p>Select to copy all the files in the following folder path:  <b>&lt;SiteScope root directory&gt;\templates.post.</b></p>

GUI Element	Description
<b>OS Template Browsable Files</b>	Select to copy all the files in the following folder path: <SiteScope root directory>\templates.os\browsable.
<b>OS Template Files</b>	Select to copy all the files in the following folder path: <SiteScope root directory>\templates.os.
<b>Mail Reports Template Files</b>	Select to copy all the files in the following folder path: <SiteScope root directory>\templates.history.
<b>Mail Template Files</b>	Templates that can be selected when creating an email alert action.  Select to copy all the files in the following folder path: <SiteScope root directory>\templates.mail.
<b>Sound Template Files</b>	Templates that can be selected when creating a sound alert action. They include the media files that create the sound for a triggered alert.  Select to copy all the files in the following folder path: <SiteScope root directory>\templates.sound.
<b>Scripts Remote Files</b>	Select to copy all the files in the following folder path: <SiteScope root directory>\scripts.remote.
<b>Scripts Files</b>	Scripts that can be selected when creating a script alert action.  Select to copy all the files in the following folder path: <SiteScope root directory>\scripts.
<b>MIB Files</b>	Select to copy all the files in the following folder path: <SiteScope root directory>\templates.mib.

 **Select Instances to Sync**

<b>Description</b>	This page displays a tree with all the instances of the type of file or object selected in the Select Types to Sync page. You can then select specific instances of the file type or object type you want copied from the source SiteScope to the target SiteScopes.
<b>Important Information</b>	<ul style="list-style-type: none"><li>▶ You can use the <b>Select All</b>, <b>Clear Selection</b>, and <b>Invert Selection</b> buttons to modify your selection of file or object instances.</li><li>▶ When you finish making your selections, click <b>Finish</b>.</li></ul>
<b>Wizard Map</b>	The Sync SiteScopes wizard includes: Sync SiteScopes Wizard - Select Source and Targets Page > Select Types to Sync > <b>Select Instances to Sync</b> > Summary Page.



The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Files/objects tree>	<p>Use the tree to select or clear specific instances occurring in the source SiteScope of the file type or object type you want to copy to the target SiteScope. The tree lists all instances of the selected file type or object type that occur in the source SiteScope.</p> <p><b>Default value:</b> All instances of every file or object selected in the Select Types to Sync page are selected. Clear the check box next to an instance to remove it from the sync operation.</p>
<b>Override existing instances</b>	<p>Select this option for the sync action to override any instances of the same name in the target SiteScopes with the selected instances.</p> <p>If this option is cleared and during the sync operation, an instance of the object or type with the same name is found in the target, the sync operation does not copy the instance onto the target SiteScope.</p> <p><b>Example:</b> You selected Absolute Schedule Preferences in the Select Type to Sync page and the target SiteScope has an absolute schedule with the same name as in the source SiteScope:</p> <ul style="list-style-type: none"> <li>➤ If this option is selected, the target's absolute schedule is overwritten with the properties of the schedule in the source SiteScope.</li> <li>➤ If this option is cleared, the target's absolute schedule maintains its properties and is not overwritten.</li> </ul>

## Summary Page

<b>Description</b>	Displays the number of objects or files successfully copied to the target SiteScopes. If any objects or files failed to copy to the target SiteScopes, this number is also displayed.
<b>Wizard Map</b>	The Sync SiteScopes wizard includes: Sync SiteScopes Wizard - Select Source and Targets Page > Select Types to Sync > Select Instances to Sync > <b>Summary Page</b> .

## Troubleshooting and Limitations

Use the following information to troubleshoot issues, as required.

### **Receive a 408 error when attempting to access SiteScope user interface from System Availability Management Administration.**

**Possible Solution 1:** Add the SiteScope machine's URL to your Web browser's list of trusted sites and restart all browsers.

**Possible Solution 2:** Configure the browser to accept cookies from the SiteScope server.

### **Reverse integration does not work.**

**Possible Solution:** Enter the SiteScope machine name in the **SiteScope agent machine location** field when adding a SiteScope to System Availability Management.

## **Page cannot be displayed due to 404 error.**

This error may occur because there is no access from the browser machine to SiteScope (pinging the machine also does not work). The SiteScope host may be changed to a fully qualified host name after adding the SiteScope to System Availability Management Administration.

**Possible Solution:** If there is no DNS configured for the network, you can configure SiteScope to report its IP address to HP Business Availability Center. Open the <SiteScope root directory>\groups\master.config file, and enter the SiteScope machine's IP address in the `_sisHostNameOverride` property.

To solve the problem on the browser's machine, you can add the SiteScope machine name with IP to the host's file in the `//WINDOWS/system32/drivers/` directory on the HP Business Availability Center machine.

## **Flash components (summary graphs) are not displayed in the System Availability Management Administration page.**

**Possible solution:** Install Flash on the client browser.

## **Error while adding a SiteScope to System Availability Management Administration in the Add SiteScope page.**

While adding the SiteScope to System Availability Management Administration, an error occurs and you want to change the **Display name** field to try to add the SiteScope again. The **Profile name** field, which is used in Business Availability Center reports, Dashboard, and so forth, is defined from the **Display name** field. The **Profile name** may still have the default value from the first time you tried adding the SiteScope.

**Possible solution:** If you change the **Display name** field or **Host name** field after an error during initially trying to add the SiteScope, you should change all the fields that get their default values from those fields, for example **Profile name**.

### **Error while opening the SiteScope user interface when SiteScope is unable to access the HP Business Availability Center permissions application.**

The following error message is displayed: "The SiteScope interface failed to open because SiteScope was unable to access the HP Business Availability Center's permissions application using http://<your BAC server>/topaz/ url. SiteScope needs this access to build the permission model before granting access to the SiteScope interface. Check your network configuration and verify that SiteScope can access HP Business Availability Center."

**Possible Solution 1:** Check your network configuration.

**Possible Solution 2:** Add the IP address of the HP Business Availability Center server to the `etc\hosts` file on the SiteScope machine.

### **Javascript errors while opening specific features in a SiteScope hosted from HP Business Availability Center when using a Firefox 2.x browser.**

When SiteScope is hosted from HP Business Availability Center, the following features may not work when using a Firefox 2.0.x browser: Opening help pages, diagnostic tools, reports, copying between SiteScopes, Monitor Deployment Wizard, Link Monitor to CI, and the Publish Templates PDF report.

**Possible Solution:** Use Firefox 3.x or an Internet Explorer browser.

# 5

---

## Integrating with HP Business Availability Center

This chapter includes the main concepts, tasks, and reference information for integrating SiteScope with HP Business Availability Center.

### **This chapter includes:**

#### Concepts

- ▶ Understanding SiteScope Integration with HP Business Availability Center on page 150
- ▶ Configuring the Integration on page 152
- ▶ Integrating SiteScope Data with HP Business Availability Center's Configuration Items on page 155
- ▶ Reporting Discovered Topologies to HP Business Availability Center on page 160
- ▶ Accessing SiteScope and Building Permissions Model on page 163

#### Tasks

- ▶ Collect Data on the Performance of an IT Resource on page 164

#### Reference

- ▶ Monitors Without Host Data on page 168

**Troubleshooting and Limitations** on page 170

## Understanding SiteScope Integration with HP Business Availability Center

---

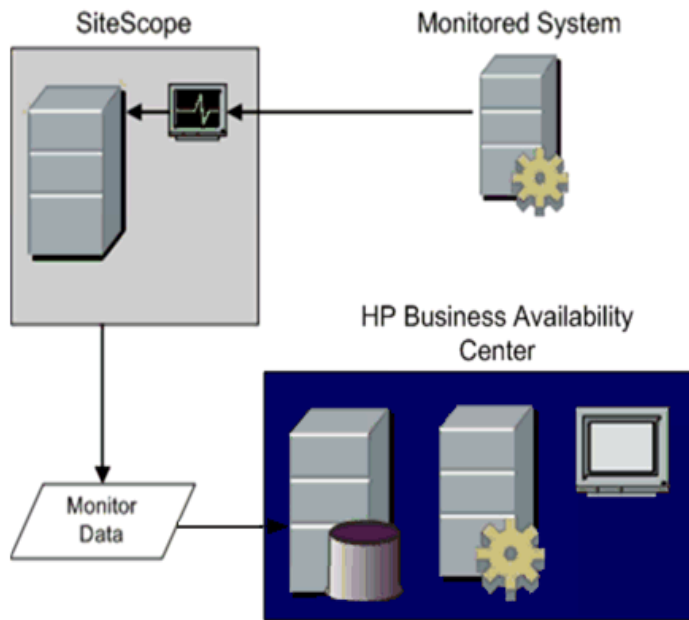
**Note:** This section is relevant only to those users integrating SiteScope with HP Business Availability Center.

---

SiteScope, as a standalone application, is an agentless solution for IT infrastructure performance and availability monitoring. SiteScope can also be used as a data collector for HP Business Availability Center. HP Business Availability Center collects data about end-users, business processes, and systems.

When configured as a data collector to HP Business Availability Center, the data and measurements collected by SiteScope monitors can be passed on to HP Business Availability Center for use in reports and analysis. Monitor data can be sent for all monitors or for selected monitors.

The following diagram illustrates the use of SiteScope as a data collector for HP Business Availability Center.



HP Business Availability Center includes a System Availability Management Administration page. This function allows you to manage SiteScope monitor configurations for one or more SiteScope servers through a central console. This level of SiteScope integration is separate from the integration of SiteScope monitor data with HP Business Availability Center.

The following table displays the HP Business Availability Center releases that are compatible with SiteScope 10.10.

HP SiteScope Version	HP Business Availability Center Version			
	8.01	8.00	7.50	7.0
SiteScope 10.10	Recommended	Supported	Supported	Supported

## **Configuring the Integration**

To enable the integration between SiteScope and Business Availability Center, the SiteScope must be configured as a data collector for Business Availability Center. This involves adding a SiteScope to the System Availability Management Administration page in the Business Availability Center. For details on this task, see “Collect Data on the Performance of an IT Resource” on page 164.

If the HP Business Availability Center Server to which you are connecting is on a different machine than the HP Business Availability Center Server to which SiteScope reports data, you must provide connection information for both servers under the **Main Settings** in SiteScope’s Integration Preferences, or under **Distributed Settings** in System Availability Management Administration’s New SiteScope Page.

Monitors created in SiteScope before registration to Business Availability Center have their logging option set to **Disable reporting to BAC**. After you configure SiteScope as a data collector reporting to Business Availability Center, the default for new monitors created in SiteScope is to log their monitoring data to Business Availability Center.

To change logging options, edit a specific monitor and select the relevant option in the **HP BAC Integration Settings** panel of the monitor properties page. For details, see “HP BAC Integration Settings” on page 370. You can use the Global Search and Replace wizard to update the logging options on those monitors created before the integration was established. For details on the wizard, see “Global Search and Replace” on page 171.

This section includes the following topics:

- ▶ “Using SSL for SiteScope-HP Business Availability Center Communication” on page 153
- ▶ “Changing the Gateway Server to Which SiteScope Sends Data” on page 154



## Using SSL for SiteScope-HP Business Availability Center Communication

You can use Secure Sockets Layer (SSL) to transmit data from SiteScope to the Business Availability Center server. If you have installed a certificate signed by a root Certificate Authority on the Business Availability Center server, no additional setup is required on the SiteScope server. If you are using a self-signed certificate on the HP Business Availability Center server and want to use that certificate for secure communication with SiteScope, you must perform the steps as described in “Use SSL for SiteScope-HP Business Availability Center Communication” on page 1424.

---

### Note:

- ▶ You must specify these settings only if the certificate installed on the Business Availability Center machine is not signed by a root Certificate Authority (CA). For example, if you are using a certificate signed by a Certificate Authority like Verisign, you do not need to change these settings.
  - ▶ You can import the self-signed certificate into the same keystore file used for other SiteScope monitors but that is not required. You can create a separate keystore for the Business Availability Center server certificate.
-

## Changing the Gateway Server to Which SiteScope Sends Data

You can change the Gateway Server to which a SiteScope reports its data. Generally, this is only applicable if you are working with an HP Business Availability Center deployment with components installed on more than one server. You make this change by entering the required Gateway Server name or IP address in the **Business Availability Center server machine name/IP address** box in the Integration Preferences page. You must also update the SiteScope settings with the Gateway Server name in System Availability Management Administration.

---

**Note:** This function can only be used for changing the Gateway Server for a SiteScope that is already registered with a given HP Business Availability Center installation. It cannot be used to add a new SiteScope, or to connect a SiteScope to a different HP Business Availability Center system.

---

For information about troubleshooting reporting data to HP Business Availability Center, see “Troubleshooting and Limitations” on page 170.

For details on configuring these preferences, see “Integration Preferences User Interface” on page 1429.

## Integrating SiteScope Data with HP Business Availability Center's Configuration Items

---

**Note:** This section is relevant only to those users integrating SiteScope with HP Business Availability Center.

---

When a monitor instance is added to a SiteScope reporting data to Business Availability Center, that monitor creates a corresponding configuration item (CI) in the HP Universal CMDB. For details on understanding configuration items, see “Configuration Items (CI)” in *Model Management* in the HP Business Availability Center Documentation Library.

The SiteScope monitors that populate the Universal CMDB include both actual monitors and the groups in which they are created. Actual monitors instances are represented in the Universal CMDB as monitor CIs. Monitor CIs receive data from the corresponding SiteScope monitor instance and use the data to calculate Key Performance Indicator (KPI) status. SiteScope groups are represented as group CIs in the Universal CMDB and receive KPI status from the monitor CIs created by the monitors they are running.

This section includes the following topics:

- “Monitor Types and Topology Reporting” on page 156
- “Creating Relationships Between Monitors and CIs” on page 157
- “Aging of CIs in CMDB” on page 158
- “Discovery Scripts and the Package Manager” on page 159

## Monitor Types and Topology Reporting

SiteScope reports different levels of topology data to the CMDB depending on the type of monitor and the options selected for the monitor. The types of monitors are as follows:

- ▶ **Technology Integration Monitors.** These monitors report data based on the topology settings script you select and edit for the monitor. The data they report is tightly integrated with Business Availability Center. You can create a custom topology or use a predefined script to forward the relevant data. For details on these monitors and how to work with their topology settings, see “Topology Settings for Technology Integration Monitors” on page 1133.
- ▶ **Monitors of Supported Environments.** For these supported environments SiteScope acts like a discovery probe when the monitor is created or its configuration is changed. When the **Include topology data when reporting to BAC** option under the **HP BAC Integration Settings** pane is selected, SiteScope automatically discovers the application’s topologies and populates the CMDB with the relevant CIs and monitor CIs. For details and a list of supported environments, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160.
- ▶ **Monitors of Hosts.** These are monitors that are not included among the Technology Integration monitors or the monitors of supported environments but can forward host topology data to Business Availability Center. When the **Include topology data when reporting to BAC** option under the **HP BAC Integration Settings** pane is selected, SiteScope forwards the host topology along with monitor CI data to Business Availability Center. For details on this option, see “HP BAC Integration Settings” on page 370.
- ▶ **Monitors Without Host Data.** SiteScope includes monitors that do not monitor hosts or servers and, therefore, cannot report host data to the CMDB. These monitors do not have the option to include topology data when reporting to Business Availability Center. For a list of these monitors, see “Monitors Without Host Data” on page 168.

## Creating Relationships Between Monitors and CIs

You can also create relationships between SiteScope monitor CIs and existing CIs in the Universal CMDB. This relationship enables the monitor to pass KPI status to the CI to which it is attached, even if that CI was not created from a topology forwarded by SiteScope.

This relationship can be created:

- ▶ In System Availability Management Administration, by using the **Monitor Deployment Wizard** which uses the existing CI property data in the CMDB to deploy SiteScope monitors, groups, and remote servers. For details on using the wizard, see “Monitor Deployment Wizard Overview” on page 1812.
- ▶ In IT Universe Manager, by SiteScope sending host data to Business Availability Center and connecting those hosts using the **Monitored by** relationship in IT Universe Manager. This creates a logical dependency between the CI and the monitor CI. For details, see “Working with Relationships” in *Model Management* in the HP Business Availability Center Documentation Library.
- ▶ In SiteScope, by manually selecting the **Link Monitor to CI** option when editing a monitor instance. This creates a logical dependency between the CI and the monitor CI. This option is available only when accessing SiteScope from System Availability Management Administration and when editing a monitor. It is not available when creating a monitor instance. For details on this option, see “Link Monitor to CI” on page 369.

## Aging of CIs in CMDB

In the CMDB, CIs that have had no activity over a period of time are removed from the database. The CIs created from SiteScope data are also subject to this aging policy. However, SiteScope prevents the CIs it has sent to Business Availability Center from being removed by synchronizing the data it sends to Business Availability Center. When this synchronization occurs, it refreshes the data for those CIs and creates activity on the CIs.

For details on setting the time interval for topology synchronization, see “Topology Settings” on page 137. For details on the Aging Mechanism, see “Working with CIs” in *Model Management* in the HP Business Availability Center Documentation Library.

---

### Note:

- ▶ Synthetic monitors and groups created by the EMS integration monitors that use Measurement field mapping are subject to the aging process regardless of the synchronization.
  - ▶ If you delete a CI from CMDB you must perform a resynchronization or a hard synchronization of SiteScope (in Integration Preferences), or you must wait for a restart of SiteScope so the CI is restored to the CMDB. This is due to the CI cache in SiteScope that prevents SiteScope from sending an unchanged CI twice. For details, see “BAC Preferences Available Operations” on page 1436.
-

## Discovery Scripts and the Package Manager

---

**Note:** This section applies to users integrating with Business Availability Center version 8.00 or later. When integrating topology data with previous versions of Business Availability Center, SiteScope uses legacy scripts which are stored on the SiteScope server.

---

The scripts that enable SiteScope to act as a discovery probe are stored on the Business Availability Center server in the **SiteScope** package. When SiteScope is configured to discover an application's topology, SiteScope downloads the appropriate script from the Business Availability Center server. It then uses the script to perform the discovery while monitoring the application.

The SiteScope package includes scripts and other SiteScope-related CMDB resources, such as views and enrichments. You can access this package in Business Availability Center in **Admin > Universal CMDB > Settings > Package Manager**. The package is a factory package, meaning that the out-of-the-box configurations for the package enable it to perform the discoveries in SiteScope. For details on working with packages, see “Package Administration Overview” in *Model Management* in the HP Business Availability Center Documentation Library.

---

**Note for advanced users only:** Advanced users may want to modify the topology scripts within the package. Be warned that the **SiteScope** package uses scripts from other packages which may be shared by SiteScope and Discovery and Dependency Mapping. Any changes made to the scripts in the package can also affect Discovery and Dependency Mapping.

Any changes made to the topology script that influence the way a topology is reported to Business Availability Center can affect all the applications that use those topologies, including Business Availability Center applications and HP Operations Manager *i*.

---

## Reporting Discovered Topologies to HP Business Availability Center

---

**Note:** This section is relevant only to those users integrating SiteScope with HP Business Availability Center, and only when the SiteScope is reporting to HP Business Availability Center version 7.50 or later.

---

SiteScope can act as a discovery probe and discover the hierarchy of the monitored entities of selected environments. These hierarchies are represented by topologies that SiteScope reports to HP Business Availability Center. The CIs within the topologies correspond to the hosts, servers, and applications that SiteScope monitors, and are created in HP Business Availability Center's CMDB. Monitor and measurement CIs are also created and SiteScope reports their status to Business Availability Center. The relationships between the CIs are defined by the topology reported by SiteScope.

You enable this feature by selecting the **Include topology data when reporting to BAC** option under the **HP BAC Integration Settings** pane when creating or configuring a monitor instance. If this option is cleared, the CIs that were created in the CMDB are not automatically deleted. If there is no activity on the CI, they are eventually removed from the database through aging or they must be manually deleted.



## Supported Environments

This direct integration between SiteScope and Business Availability Center is available only for selected environments and with specific versions of Business Availability Center. For details on the specific topologies SiteScope reports for the applicable monitors, see:

### Database environments:

(Available when integrating with Business Availability Center version 8.00 and higher.)

- “DB2 8.x and 9.x Topology Settings” on page 496
- “Microsoft SQL Server Topology Settings” on page 673
- “Oracle Database Topology Settings” on page 759

### ERP/CRM application environments:

(Available when integrating with Business Availability Center version 7.50 and higher.)

- “SAP CCMS Topology Settings” on page 790
- “SAP Work Processes Topology Settings” on page 824
- “Siebel Application Server Topology Settings” on page 859
- “Siebel Web Server Topology Settings” on page 875

### SOA environments:

(Available when integrating with Business Availability Center version 7.50 and higher.)

- “Web Service Topology Settings” on page 1053

**Web server environments:**

(Available when integrating with Business Availability Center version 7.50 and higher.)

- “Microsoft IIS Server Topology Settings” on page 667
- “WebLogic Application Server Topology Settings” on page 580
- “WebSphere Application Server Topology Settings” on page 1073

**Virtualization environments:**

(Available when integrating with Business Availability Center version 8.02 and higher.)

- “Solaris Zones Topology Settings” on page 909
- “VMware Performance Topology Settings” on page 1018

For details on the Topology Settings user interface, see “Topology Settings” on page 137.

## Accessing SiteScope and Building Permissions Model

---

**Note:** This section is relevant only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center, and only when the SiteScope is reporting to HP Business Availability Center version 7.00 or later.

---

System Availability Management Administration builds a permissions model for each Business Availability Center user accessing SiteScope. That permissions model is based on the Business Availability Center user's permissions for SiteScope objects and not on the user's permissions as defined in SiteScope.

When assigning permissions to users in Business Availability Center for accessing a SiteScope through System Availability Management Admin, be aware that the permissions in Business Availability Center have been mapped to the equivalent permissions in SiteScope. The permissions model maps between the types of permissions available in SiteScope to what can be granted in Business Availability Center.

There are several differences between the Business Availability Center permissions model and SiteScope standalone permissions:

- ▶ Business Availability Center permissions enables granting permissions per group instance. In SiteScope standalone, permissions are granted onto groups as an object and do not have the instance granularity that exists in Business Availability Center.

For example, a user can have permissions within Business Availability Center to view or change specific instances of SiteScope groups with no permission to access other SiteScope groups.

- ▶ SiteScope enables specific types of permissions onto object types, such as the ability to enable/disable whereas in Business Availability Center the operations are standard for all objects and include view, change, add, and full control. In this case, enable/disable is mapped to Business Availability Center's change permission.

- ▶ When applying permissions in Business Availability Center onto SiteScope objects, you can hover over an operation to see a description of how it maps to the permissions available to users of SiteScope standalone.
- ▶ Only a user at the Administrator level in SiteScope standalone has the necessary permissions to add a SiteScope to System Availability Management Administration in Business Availability Center.

## Collect Data on the Performance of an IT Resource

---

**Note:** This section is relevant only to those users integrating SiteScope with HP Business Availability Center.

---

This task describes how to set up and use SiteScope to collect data on the performance of IT infrastructure components.

This task includes the following steps:

- ▶ “Prerequisites” on page 165
- ▶ “Download and Install SiteScope” on page 165
- ▶ “Integrate the Installed SiteScope with Business Availability Center” on page 165
- ▶ “Configure SSL for SiteScope-HP Business Availability Center Communication” on page 166
- ▶ “Configure SiteScope Groups and Subgroups” on page 166
- ▶ “Configure SiteScope Monitors” on page 167
- ▶ “Assign Permissions in Business Availability Center” on page 167
- ▶ “Modify the Integration Settings - Optional” on page 168

## 1 Prerequisites

Prepare a plan that maps out the specific IT infrastructure resources who data you want to collect. Include information about the business processes that are affected by the specified infrastructure components. For example, business processes being monitored by Business Process Monitor, that are running on an application server against which you plan to run SiteScope monitors.

## 2 Download and Install SiteScope

Navigate to **Admin > Platform > Setup and Maintenance**, click **Downloads**. Download and save the SiteScope installation files (for Windows or Solaris) to a local or network drive.

Install SiteScope on machines designated to run the SiteScope data collector. You can run multiple SiteScopes from multiple platforms. For more information, see the *HP SiteScope Deployment Guide* PDF.

## 3 Integrate the Installed SiteScope with Business Availability Center

In Business Availability Center, navigate to **Admin > System Availability Management**.

Add the SiteScope to System Availability Management Administration. For details on the user interface, see “New SiteScope Page” on page 133.

For details on this topic, see “System Availability Management Administration Overview” on page 120.

**Note:**

- ▶ If you are working with a SiteScope that is not accessible to Business Availability Center (for example in HP Software-as-a-Service), the procedure for the integration includes creating an empty profile in System Availability Management Administration and creating an Integration Preference for BAC in SiteScope. For details on how to perform this task, see “Configure SiteScope-HP Business Availability Center Integration Preferences for Inaccessible Profiles” on page 1423.
  - ▶ When working under high load, you should suspend all monitors before connecting to HP Business Availability Center for the first time.
- 

#### **4 Configure SSL for SiteScope-HP Business Availability Center Communication**

For details on this task, see “Use SSL for SiteScope-HP Business Availability Center Communication” on page 1424.

#### **5 Configure SiteScope Groups and Subgroups**

Create groups and subgroups to organize the monitors to be deployed. For example, you can create groups of locations, server types, network resources, and so forth.

For details on the user interface, see “New SiteScope Group Dialog Box” on page 297.

## 6 Configure SiteScope Monitors

When configuring monitors, verify that HP BAC Logging settings are set as required. You can create monitors individually into the groups you created or in the following ways:

- ▶ Using the Monitor Deployment Wizard to deploy monitors onto existing CIs in the CMDB. For details on this topic, see “Monitor Deployment Wizard Overview” on page 1812.
- ▶ Using Solution Templates to configure predefined sets of monitors on specific systems. For details on this topic, see “SiteScope Solution Templates” on page 1665.
- ▶ Using SiteScope templates. For details on this topic, see “SiteScope Templates Overview” on page 1558.

Once defined, the SiteScope and its groups and monitors are added as CIs to the CMDB and are automatically attached to the relevant monitor views, from where they can be added to other views. When editing a monitor in System Availability Management Administration, you can associate the monitor with existing CIs using **Link Monitor to CI Settings**. For example, you can attach the CPU monitor to an existing logical CI representing a machine whose CPU is being monitored.

The data from the SiteScope is available in Dashboard and Service Level Management.

## 7 Assign Permissions in Business Availability Center

Navigate to **Admin > Platform > Users and Permission**, click **User Management**.

For each defined user, assign permissions to view SiteScope groups and their subgroups in System Availability Management reports and custom reports. For details, see “System Availability Management Administration (SAM Admin)” in *Platform Administration* in the HP Business Availability Center Documentation Library.

For details on how permissions are applied, see “Accessing SiteScope and Building Permissions Model” on page 163.

## 8 Modify the Integration Settings - Optional

Once you have created the integration, you can modify the settings either in SiteScope or in Business Availability Center, depending on the setting that you are modifying.

- ▶ In SiteScope, open the **Preferences** context and select **Integration Preferences**. Edit the BAC Integration Preference.

For details on the user interface, see “New/Edit BAC Integration Dialog Box” on page 1432.

- ▶ In Business Availability Center, select **Admin > System Availability Management**. In the list of SiteScopes, right-click the relevant SiteScope and select **Edit SiteScope** from the context menu.

For details on the user interface, see “New SiteScope Page” on page 133.

## Monitors Without Host Data

Following is a list of those monitors that do not monitor the status of a host or server. These monitors cannot report host CI information to Business Availability Center. Therefore, these monitors do not have the option to **Include topology data when reporting to BAC** under the **HP Integration Settings** pane. The monitors include:

- ▶ Composite Monitor
- ▶ Directory Monitor
- ▶ e-Business Transaction Monitor
- ▶ File Monitor
- ▶ Formula Composite Monitor
- ▶ JMX Monitor (when not monitoring WebLogic)



- Link Check Transaction Monitor
- Log File Monitor
- Microsoft Windows Dial-up Monitor
- Microsoft Windows Media Player Monitor
- Multi Log File Monitor
- Network Bandwidth Monitor
- Real Media Player Monitor
- Script Monitor
- SNMP Trap Monitor
- URL Monitor
- URL Content Monitor
- URL List Monitor
- URL Sequence Monitor
- Web Script Monitor
- Web Service Monitor
- XML Metrics Monitor

## Troubleshooting and Limitations

### Reporting Data to Business Availability Center

Due to the complexity of some monitoring deployments and network communications, there SiteScope may be temporarily unable to communicate with the Business Availability Center server. SiteScope Health monitoring includes several monitors for watching connectivity and data transfers to the Business Availability Center server.

If SiteScope is unable to connect to the HP Business Availability Center Server, SiteScope continues to record and store monitor data files locally. Once the number of data files exceeds a specified threshold, SiteScope saves the data files in a cache folder with the syntax `<SiteScope_root>\cache\persistent\topaz\data<index>.old`.

---

**Note:** By default, the threshold number of data files is set to 1,000 files. You can change this setting by modifying the `_topazMaxPersistenceDirSize` property in the `master.config` file.

---

After the connection between SiteScope and the Agent Server is restored, you must manually copy the files from these folders to the `<SiteScope root directory>\cache\persistent\topaz\data` folder. We recommend that you only copy these files when the data folder is empty to avoid overloading the system with large amounts of data to upload. When the number of `data.old` folders exceeds a specified threshold, by default 10 folders, the oldest folders are deleted.

---

**Note:** You can configure the number of `data.old` folders to keep by modifying the `_topazMaxOldDirs` property in the `master.config` file.

---

# 6

---

## Global Search and Replace

This chapter includes the main concepts, tasks, and reference information for the Global Search and Replace Wizard.

### **This chapter includes:**

#### Concepts

- ▶ Global Search and Replace Overview on page 171

#### Tasks

- ▶ Perform a Global Search and Replace on page 174

#### Reference

- ▶ Global Search and Replace User Interface on page 178

### **Global Search and Replace Overview**

The Global Search and Replace Wizard enables you to make changes to monitor, alert, alert action, group, preferences, and report properties. You can select an object based on object type and globally replace any of the properties of the selected object across your SiteScope or across multiple SiteScopes when working in System Availability Management Administration.

For example, when upgrading HP Business Availability Center, use the Global Search and Replace Wizard to configure all the SiteScopes reporting data to Business Availability Center to the upgraded version.

This section contains the following topics:

- “Filter Affected Objects” on page 172
- “Replace Versus Find and Replace” on page 172
- “Threshold Settings” on page 173

### **Filter Affected Objects**

Use the Filter Affected Options option to further refine your selected object for the search operation. You can select specific properties and select or enter values pertaining to your object. This enables you to limit the selected objects but not the value to replace.

When performing the replace operation, only the value to replace is replaced and only on those objects that match the properties selected in the Filter Affected Options page. For example, select all monitors with frequency set to 5 minutes and replace the monitor dependency setting for all of those monitors, or select only those monitors monitoring a specific server and replace the threshold settings for only those monitor instances matching the value of the server entered in the filter.

### **Replace Versus Find and Replace**

Use the replace method to search for a field value and replace it with a new value. For example, change the default monitor run frequency setting for the selected monitors by selecting the **Frequency** check box in the Monitor Run Settings area, and updating the frequency value from 10 to 15 minutes.

Use the find and replace method to search for specific settings and property values and replace only those objects with the entered setting or value. You can search a string, value, or regular expression pattern and replace only that string. Replacements are made only if the filter criteria matches. For example, search for all monitors whose name value includes a server name that is no longer in use. Replace the string representing the old server with a new string representing the updated server.

## Threshold Settings

When replacing threshold settings for monitors, by default you replace only those settings that share all of the following:

- ▶ have the same condition (**Error if**, **Warning if**, or **Good if**)
- ▶ are configured for the same schedule
- ▶ use the same operator type (< <=, > >=, ==, !=, contains, !contains).

---

**Note:** < (less than) and <= (less than and equal to) are considered the same operator type as are > (greater than) and >= (greater than and equal to).

---

You also have the option to override all the existing threshold settings that have the same condition (**Error if**, **Warning if**, or **Good if**) regardless of the operator used and the schedule configured. The option is called **Override Category** and appears in the Choose Changes page of the wizard under the **Threshold Settings** area if you selected **Monitor** in the Select Type page of the wizard.

For example, you want to change the **Error if** threshold settings for all CPU monitors to greater than 85%. In the wizard, you select **Monitor** in the Select Type page, **CPU** in the Select Subtype page, and expand the **Threshold Settings** area in the Choose Changes page.

If you select the **Override Category** option when selecting greater than 85% as the **New Error if** status condition, all the existing **Error if** settings for all CPU monitors are overwritten and changed to greater than 85% when you complete the wizard.

If you leave the option cleared, the greater than 85% **Error if** setting you select in the wizard replaces only those **Error if** settings that use the < (greater than) and <= (greater than and equal to) operators and were configured for the same schedule for all CPU monitors.

For details on setting thresholds, see “Setting Status Thresholds” on page 309.

## Perform a Global Search and Replace

This task describes how to perform a global search and replace for objects, using the Global Search and Replace Wizard.

This task includes the following steps:

- “Begin Running the Global Search and Replace Wizard” on page 174
- “Select SiteScope” on page 174
- “Select Object Type” on page 175
- “Search and Replace Objects” on page 175
- “Check Affected Objects” on page 177
- “Review Replaced Objects” on page 178

### 1 Begin Running the Global Search and Replace Wizard

When you are accessing SiteScope from Business Availability Center, in System Availability Management Administration, select **Admin > System Availability Management** and click the **Global Search and Replace** button.

When you are accessing SiteScope standalone, right-click SiteScope root or the group or monitor in the monitor tree to which you want to perform the global replace. To replace Preferences objects, right-click SiteScope root. To replace alert objects, right-click SiteScope root, or the relevant group or monitor object. Select **Global Search and Replace** from the context menu.

For details on the user interface, see “Global Search and Replace Wizard” on page 178.

### 2 Select SiteScope

---

**Note:** This step is only applicable when you access the Global Search and Replace wizard from System Availability Management.

---

In the **Select SiteScope** page, select one or more SiteScopes on which to run the search and replace.

### 3 Select Object Type

In the **Select Type** and **Select Subtype** page, select the object and, if relevant, the subtype upon which you want to make a replacement.

For details on the user interface, see “Select Type Page” on page 180 and “Select Subtype Page” on page 181.

#### Example

You want to change the threshold boundaries for all CPU monitors.

You select **Monitor** as the object type.

You select **CPU** as the specific monitor type.

### 4 Search and Replace Objects

In the **Replace Mode** page, select the type of replacement. Select **Replace** to globally replace the object or select **Find and Replace** to replace specific instances of the object. In the **Choose Changes** page, you select what properties or values to replace.

For details on the user interface, see “Replace Mode Page” on page 181 and “Choose Changes Page” on page 183.

### Example - Setting Up Alert Action to Send Alert Messages to Specified Email Addresses

You set up your alert action to send alert messages to specified email addresses. However, one of the email addresses you configured to receive the alerts has changed and you want to send alert messages to the new email address. You want to update only the email address that has changed.

After selecting **Alert Action** as the object type, you select **Find and Replace** in the Replace Mode page.

<p>Select Type</p> <p>Select Subtype</p> <p>► Replace Mode</p> <p>Choose Changes</p> <p>Affected Objects</p> <p>Review Summary</p> <p>Summary</p>	<p><b>Replace Mode</b></p>
	<p>Select the replace mode. Choose Replace if you want to replace a field with a new value. Choose Find and Replace to search for a string with a field and replace it with a new value.</p> <p> <input type="radio"/> Replace  <input checked="" type="radio"/> Find And Replace                 </p>

In the Choose Changes page, you enter the old email address in the **Find** field and the new email address in the **and Replace with** field.

<p>Select Type</p> <p>Select Subtype</p> <p>Replace Mode</p> <p>► Choose Changes</p> <p>Affected Objects</p> <p>Review Summary</p> <p>Summary</p>	<p><b>Choose Changes</b></p>
	<p>Enter the changes that you want to perform. Every marked property will be replaced by the entered value.</p> <p>Find: <input type="text" value="@yahoo.com"/> and replace with: <input type="text" value="@hotmail.com"/></p> <p>General Settings <span style="float: right;">▼</span></p> <p>Alert Targets <span style="float: right;">▲</span></p> <p><input type="checkbox"/> Alert Targets</p>



## 5 Check Affected Objects

In the **Affected Objects** page, view the affected objects and, if necessary, clear or select objects for the replacement operation. Optionally, you can open the Filter Affected Objects dialog box to filter by the object properties. Here you select on which objects to perform the replace operation.

For details on the user interface, see “Affected Objects Page” on page 186.

### Example - Reducing the Frequency of a Monitor Run on a Specific Server

You want to reduce the frequency of how often a monitor runs on a specific server in your company.

In the Choose Changes page, you then enter a new frequency of once a day, to monitor the specified server.

You then filter your selection in the Filter Affected Objects page to include only those monitors monitoring the specified server.

## 6 Review Replaced Objects

In the **Review Summary** page, review the results of the replacement operation and click **Finish** to complete the wizard. You can view a summary of the changes in the **Summary** page to see which changes were implemented successfully and in which errors occurred.

For details on the user interface, see “Review Summary Page” on page 188 and see “Summary Page” on page 190.

## Global Search and Replace User Interface

**This section includes:**

- ▶ Global Search and Replace Wizard on page 178

## Global Search and Replace Wizard

<b>Description</b>	<p>Global Search and Replace enables you to make changes to group, monitor, preferences, alert, alert action, and report properties. These changes can be made across a SiteScope or across several SiteScopes when working in System Availability Management Administration.</p> <p><b>To access:</b> In SiteScope standalone, right-click SiteScope root or the group or monitor in the monitor tree to which you want to perform the global replace. To replace Preferences objects, right-click SiteScope root. To replace alert objects, right-click SiteScope root, or the relevant group or monitor object. Select <b>Global Search and Replace</b> from the context menu.</p> <p>In System Availability Management Administration, select <b>Admin &gt; System Availability Management</b> and click the <b>Global Search and Replace</b> button.</p> <p><b>Note:</b> You may be prompted to enter your user login credentials when you click the <b>Help</b> button in any page of the wizard.</p>
--------------------	---

<b>Included in Tasks</b>	“Perform a Global Search and Replace” on page 174
<b>Wizard Map</b>	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

### **Select SiteScope Page**

<b>Description</b>	Use the Select SiteScope Page to select the SiteScope on which to make replacements.
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This page is displayed only when you are working in System Availability Management.</li> <li>▶ Only SiteScopes running version 9.0 and higher and whose connection status allows configuration changes from System Availability Management are listed.</li> <li>▶ You must select at least one SiteScope.</li> </ul>
<b>Wizard Map</b>	The Global Search and Replace Wizard includes: <b>Select SiteScope Page</b> (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

 **Select Type Page**

<b>Description</b>	Use the Select Type page to select the object type on which you want to make replacements.
<b>Important Information</b>	Only those types of objects available for the node you selected are listed.
<b>Wizard Map</b>	The Global Search and Replace Wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > <b>Select Type Page</b> > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Alert</b> <b>Alert Action</b> <b>Group</b> <b>Monitor</b> <b>Preferences</b> <b>Report</b>	You can select only one object type for each replace operation. Only those objects that exist in the SiteScope appear.  When performing Global Search and Replace from System Availability Management Administration, group, monitor, alert, alert action, and preferences appear only if they exist on at least one SiteScope selected in the previous page.

## Select Subtype Page

<b>Description</b>	Use the Select Subtype page to select the properties of the object type on which you want to make replacements.
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This page opens only if you selected <b>Alert Action</b>, <b>Monitor</b>, or <b>Preferences</b> as the object type in the Select Type Page of the wizard.</li> <li>▶ If you selected the object type <b>Group</b>, <b>Alert</b>, or <b>Report</b>, this page does not open.</li> </ul>
<b>Wizard Map</b>	The Global Search and Replace Wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > <b>Select Subtype Page</b> > Replace Mode Page > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

## Replace Mode Page

<b>Description</b>	Use the Replace Mode page to select the type of replacement: global replacement or replacement based on filter criteria.
<b>Wizard Map</b>	The Global Search and Replace Wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > <b>Replace Mode Page</b> > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Find and Replace</b>	<p>Select to search the target objects for properties that match a string or regular expression and replace only the matching pattern with the replacement value.</p> <p>This method of replacement includes a search for specific settings and property values and replaces only those objects with the entered setting or value. You can select only a partial value and replace only that string.</p> <p><b>Example:</b> Search for all monitors whose name value includes a server name that is no longer in use. Replace the string representing the old server with a new string representing the updated server.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ If you select this option, only settings whose values can contain a string are available in the settings area of the <b>Choose Changes</b> page and can be selected for the find and replace action.</li> <li>➤ Use this setting to determine the selection and the value to replace. It differs from the Advanced Filter option which is a way to limit the selected objects but not the value to replace.</li> </ul>
<b>Replace</b>	Globally replaces all matching objects with the new string or value.

 **Choose Changes Page**

<b>Description</b>	<p>Use the Choose Changes page to select what to replace for the global replace.</p> <p>The wizard displays only the settings and properties that may be changed for the object type selected in the previous pages.</p> <p>The filter criteria is built from your selections in the Type, Subtype, and Advanced Filter pages.</p>
<b>Important Information</b>	<p>The subtype's properties may be displayed differently than how they are displayed when editing a monitor, alert, preference, and so forth in SiteScope.</p> <p><b>Examples: Mail Preferences</b> is a text box in Global Search and Replace utility rather than a drop-down list, and the <b>Depends on</b> property is not displayed in the Global Search and Replace utility.</p> <p><b>Note:</b> You cannot use the wizard to make changes to a monitor's Enable/Disable Monitor settings. Use the <b>Enable/Disable Monitors</b> button in the Dashboard instead.</p> <p><b>Note for users of SiteScope within System Availability Management Administration:</b> If the SiteScopes selected for the replace operation are not all the same version, the subtypes of the SiteScopes may have different properties.</p>
<b>Wizard Map</b>	<p>The Global Search and Replace Wizard includes:</p> <p>Select SiteScope Page (when working in System Availability Management Admin) &gt; Select Type Page &gt; Select Subtype Page &gt; Replace Mode Page &gt; <b>Choose Changes Page</b> &gt; Affected Objects Page &gt; (Filter Affected Objects Dialog Box) &gt; Review Summary Page &gt; Summary Page.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Settings area>	<p>This area includes the settings for the object you selected. For details about these settings, refer to the selected object’s settings page.</p> <ul style="list-style-type: none"> <li>▶ If you selected <b>Find and Replace</b> in the Replace Mode page, you select only the setting in the settings area. Enter the old and new values to replace in the <b>Find/Replace with</b> boxes.</li> <li>▶ If you selected <b>Replace</b> in the Replace Mode page, you select the setting and the new value in the settings area.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ If you selected <b>Monitor</b> in the Select Type page, in the <b>Threshold Settings</b> area, the <b>Override Category</b> option appears. When selected, this option enables you to override the threshold settings of the same threshold condition (<b>Error if</b>, <b>Warning if</b>, or <b>Good if</b>) for the selected monitor instances with the settings you enter here for the replace operation. If this option is cleared, the settings you enter here replace only those settings with the same operator type (&lt; &lt;=, &gt; &gt;=, !=, ==, contains, !contains) and the same configured schedule for the monitor instances. Any other settings for the same condition but with a different operator type or a different schedule remain. For details on this option and an example, see “Threshold Settings” on page 173.</li> <li>▶ If you selected <b>Alert</b> in the Select Type page, the <b>Monitor type match</b> field in the Filter Settings is not displayed and its values cannot be replaced in the wizard.</li> </ul>




GUI Element	Description
<p><b>Find</b> <b>Replace With</b></p>	<p>If you chose the <b>Find and Replace</b> option in the Replace Mode page, the text boxes <b>Find</b> and <b>Replace With</b> are added to the top of this page.</p> <ul style="list-style-type: none"> <li>▶ In the <b>Find</b> box, enter the search string, value, or regular expression pattern for the setting or property you want to replace.</li> <li>▶ In the <b>Replace With</b> box, enter the string or value to which you want all matching patterns to be changed.</li> </ul> <p><b>Note:</b> If you select <b>Frequency</b> in the Monitor Run Settings, the values you enter in the <b>Find</b> and <b>Replace With</b> text boxes must be in seconds. For example, you want to find monitors with a frequency of 10 minutes and change the frequency to 20 minutes. In the <b>Find</b> text box, enter 600 and in the <b>Replace With</b> text box enter 1200.</p> <p>If no objects are found that meet the filter criteria, an error message appears. Reselect your filter criteria.</p>


 **Affected Objects Page**

<p><b>Description</b></p>	<p>Use the Affected Objects page to view the objects that you selected to change. The page displays the selected objects in tree format.</p> <p>You can clear or select objects in the Affected Objects tree for the replacement operation.</p> <ul style="list-style-type: none"> <li>▶ If you selected <b>Find and Replace</b> in the Replace Mode page, replacements are made only if the filter criteria are matched.</li> <li>▶ If you selected <b>Replace</b>, replacements are made in all selected objects.</li> </ul>
<p><b>Important Information</b></p>	<p>The objects displayed depend on whether the user has change permissions on those objects.</p> <ul style="list-style-type: none"> <li>▶ When in System Availability Management Administration, the permissions are set in Business Availability Center's Permissions Management (<b>Admin &gt; Platform &gt; Users and Permissions</b>).</li> <li>▶ When in SiteScope standalone, the permissions are set in <b>Preferences &gt; User Preferences</b>.</li> </ul>
<p><b>Wizard Map</b></p>	<p>The Global Search and Replace Wizard includes:</p> <p>Select SiteScope Page (when working in System Availability Management Admin) &gt; Select Type Page &gt; Select Subtype Page &gt; Replace Mode Page &gt; Choose Changes Page &gt; <b>Affected Objects Page</b> &gt; (Filter Affected Objects Dialog Box) &gt; Review Summary Page &gt; Summary Page.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
	<p>Optionally, click to open the <b>Filter Affected Objects</b> dialog box if you want to further refine your selections. For details on the user interface, see “Filter Affected Objects Dialog Box” on page 187.</p>
<p>&lt;Affected Objects tree&gt;</p>	<p>The Affected Objects tree includes all objects that are matched against the various filter criteria selected in the previous pages of the wizard.</p> <p>Select or clear objects as required for the replace operation.</p> <p><b>Note:</b> When using Global Search and Replace from System Availability Management Administration, a tree is displayed for each SiteScope selected.</p>

### **Filter Affected Objects Dialog Box**

<p><b>Description</b></p>	<p>Enables you to select objects based on their specific settings and not only based on object type. For example:</p> <ul style="list-style-type: none"> <li>▶ Select all alerts that have a defined category of critical and replace any setting for those alerts.</li> <li>▶ Select all groups with a dependency set to a specific monitor or group and replace any setting for those groups.</li> </ul> <p><b>To access:</b> Click the <b>Filter Affected Objects</b> button  in the Affected Objects Page.</p>
---------------------------	---

<b>Important Information</b>	Using this option only refines your selection for the replace and does not determine what to replace.
<b>Wizard Map</b>	The Global Search and Replace Wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > ( <b>Filter Affected Objects Dialog Box</b> ) > Review Summary Page > Summary Page.

The following elements are included (unlabeled GUI elements are shown in angle brackets):


GUI Element	Description
<Settings areas>	The setting areas pertinent to the object you selected are displayed. For details about these settings, refer to the selected object's settings page. Select the properties and enter the values by which to filter the selected objects.

### **Review Summary Page**

<b>Description</b>	Use the Review Summary page to preview the objects on which the replacement operation is performed.  When working with multiple SiteScopes in System Availability Management Administration, a table is displayed for each SiteScope and the name of the SiteScope appears above the table.
--------------------	---

<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The number of objects that are affected by the global replacement is displayed above the table.</li> <li>▶ Each table column can be sorted in ascending or descending order by right-clicking the column title. An up or down arrow indicates the sort order.</li> <li>▶ Once you click <b>Finish</b> in this page, you cannot undo the replacement operation.</li> </ul>
<b>Wizard Map</b>	<p>The Global Search and Replace Wizard includes:</p> <p>Select SiteScope Page (when working in System Availability Management Admin) &gt; Select Type Page &gt; Select Subtype Page &gt; Replace Mode Page &gt; Choose Changes Page &gt; Affected Objects Page &gt; (Filter Affected Objects Dialog Box) &gt; <b>Review Summary Page</b> &gt; Summary Page.</p>



The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Change the sort order in the columns by clicking the up and down arrow in the column title.</p> <p><b>Default:</b> The <b>Monitor Full Name</b> column is in alphabetical order, from top to bottom.</p>
<b>Full Name</b>	<p>Displays a tree of the monitor name and the monitor's properties whose value is being replaced.</p>
<b>Previous Value</b>	<p>The current value that changes as a result of the replace operation.</p> <p><b>Note:</b> If the value being replaced is a check box that was cleared and is now being selected, you may not see the previous value (cleared) for the check box.</p>
<b>New Value</b>	<p>The new value that you entered in the Choose Changes page.</p>

 **Summary Page**

<p><b>Description</b></p>	<p>The Summary page reports the changes that were implemented successfully and those in which errors occurred. The page displays the changes in table format.</p> <p>When working with multiple SiteScopes in System Availability Management Administration, a table is displayed for each SiteScope and the name of the SiteScope appears at the top of the table.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ There is no way to undo changes made by the replace operation.</li> <li>▶ The number of objects affected by the global replacement is given above the table.</li> <li>▶ Each table column can be sorted in ascending or descending order by right-clicking the column title. An up or down arrow indicates the sort order.</li> </ul>
<p><b>Wizard Map</b></p>	<p>The Global Search and Replace Wizard includes:</p> <p>Select SiteScope Page (when working in System Availability Management Admin) &gt; Select Type Page &gt; Select Subtype Page &gt; Replace Mode Page &gt; Choose Changes Page &gt; Affected Objects Page &gt; (Filter Affected Objects Dialog Box) &gt; Review Summary Page &gt; <b>Summary Page</b>.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Change the sort order in the columns by clicking the up and down arrow in the column title. <b>Default:</b> The <b>Monitor Full Name</b> column is in alphabetical order, from top to bottom.
<b>Full Name</b>	Displays a tree of the monitor name and the monitor's properties whose values were changed.
<b>Previous Value</b>	The value that was replaced in the global replace operation.
<b>New Value</b>	The new value that resulted from the global replace operation.
	Click to print the table. This icon appears for each table in the summary.
<b>Finish</b>	Closes the wizard. You return to SiteScope Dashboard.





# 7

---

## SiteScope Tools

This chapter includes the main concepts and reference information for SiteScope Tools.

### **This chapter includes:**

#### Concepts

- ▶ SiteScope Tools Overview on page 193

#### Tasks

- ▶ Use a Tool When Configuring or Editing a Monitor on page 195

#### Reference

- ▶ SiteScope Tools User Interface on page 196

### **SiteScope Tools Overview**

SiteScope provides a number of diagnostic tools that are useful to test the monitoring environment. You can use these tools before configuring a monitor to uncover issues and facilitate monitor configuration, and after configuring a monitor to troubleshoot and diagnose problems.


Use these tools to make a variety of requests and queries of systems you are monitoring and to view detailed results of the action. Requests may include testing network connectivity or verifying login authentication for accessing an external database or service.

Some tools are available when configuring specific monitor types to help you configure the monitor settings. You enter data into the tool fields, and have SiteScope test the data. After the data has been tested, you can apply the tested data directly to the monitor configuration form. For example, before configuring a DNS monitor, you can use the DNS Lookup Tool to translate a domain name to an IP address. After the name has been translated, you can have SiteScope apply the data to the new monitor.

For the list of SiteScope tools that are available, see “Tools Menu” on page 97.

## User Permissions

The following permissions are required to use the SiteScope tools:

- ▶ **Use tools.** To view and use the tools in the **Tools** context in the left pane, you must be an administrator in SiteScope, or a user granted **Use tools** permissions.
- ▶ **Use monitor tools.** To use a tool when configuring or editing a monitor (if a tool is available for that monitor), you must be an administrator in SiteScope, or a user granted **Use monitor tools** permissions.
  - ▶ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor.
  - ▶ When running the test tool for an existing monitor, click the **Tools**  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.

## Use a Tool When Configuring or Editing a Monitor

This task describes the steps involved in using a SiteScope tool to assist you to configure or troubleshoot a monitor.

This task includes the following steps:

- “Prerequisites” on page 195
- “Add and Configure a Monitor” on page 195
- “Configure and Run the Test” on page 195
- “Apply the Tested Data to the Monitor Fields” on page 195
- “Use a Tool to Edit or Test Monitor Properties (Optional)” on page 196

### 1 Prerequisites

Only an administrator in SiteScope, or a user granted **Use monitor tools** permissions, can use the tools that are available when configuring specific monitors.

### 2 Add and Configure a Monitor

Select **New > Monitor**, and add a new monitor from the New Monitor page. If a tool is available to help you configure the monitor, click the **Use Tool** button at the bottom of the new monitor dialog box.

### 3 Configure and Run the Test


Enter the required information in the tool dialog box, and run the tool. Any server-side validation errors are displayed in the result panel.

### 4 Apply the Tested Data to the Monitor Fields

After the configuration data has been successfully tested, click the **Apply to New Monitor** button (or **Apply to Monitor** button when editing an existing monitor) to have SiteScope apply the data to the monitor configuration.

## 5 Use a Tool to Edit or Test Monitor Properties (Optional)

You can also use SiteScope tools, where available, to edit or test configuration properties for existing monitors.

- To edit monitor configuration properties, click the **Use Tool** button in the monitor **Properties** tab, and complete steps 3 and 4.
- To open and run the tool with the monitor's existing data as its input, click the **Tools**  button in the SiteScope Dashboard toolbar. The test results are displayed in the **Results** panel. You can save the results to a file by clicking the **Save to File** button.


## SiteScope Tools User Interface

**This section includes (in alphabetical order):**

- Database Connection Tool on page 198
- Database Information Tool on page 201
- DNS Lookup Tool on page 203
- Event Log Tool on page 205
- FTP Server Tool on page 208
- LDAP Authentication Tool on page 211
- Mail Round Trip Tool on page 214
- Microsoft Windows Media Player Tool on page 218
- Network Status Tool on page 220
- News Server Tool on page 221
- Performance Counters Tool on page 223
- Ping Tool on page 226
- Processes Tool on page 228
- Real Media Player Tool on page 230
- Regular Expression Tool on page 232

- Services Tool on page 234
- SNMP Browser Tool on page 237
- SNMP Tool on page 241
- SNMP Trap Tool on page 243
- Trace Route Tool on page 245
- URL Tool on page 247
- Web Service Tool on page 251
- XSL Transformation Tool on page 258

## Database Connection Tool

<p><b>Description</b></p>	<p>The Database Connection diagnostic tool is used to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database. This diagnostic tool checks to see if:</p> <ul style="list-style-type: none"> <li>▶ the supplied database driver can be found and loaded</li> <li>▶ a connection can be made to the database</li> <li>▶ an optional SQL query can be run and the results displayed</li> <li>▶ the database connection and resources can be closed</li> </ul> <p>This tool can be useful in verifying connection parameter values needed to set up database monitors, database alerts, and database logging.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>Database Tools</b> &gt; <b>Database Connection Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the Database Counter monitor, Database Query monitor, DB2 8.x and 9.x monitor, or Technology Database Integration monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<p><b>Important Information</b></p>	<p>If exceptions or errors occur during the test, the information is printed along with suggested actions to help with troubleshooting.</p>

<b>Included in Tasks</b>	“Use a Tool When Configuring or Editing a Monitor” on page 195
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The Database Connection Tool includes the following elements:

<b>GUI Element</b>	<b>Description</b>
<b>Database connection URL</b>	<p>Enter the correct Database connection URL used when setting up the monitor. When using the Oracle thin driver, the database connection URL has the form of: jdbc:oracle:thin:@&lt;server name or IP address&gt;:&lt;port&gt;:&lt;database sid&gt;.</p> <p><b>Example:</b> To connect to the ORCL database on a machine using port 1521, enter jdbc:oracle:thin:@206.168.191.19:1521:ORCL. The colon (: ) symbol must be included as shown.</p> <p><b>Note:</b> If you want to access the database using Windows authentication, enter jdbc:mercury:sqlserver://&lt;server name or IP address&gt;:1433;DatabaseName=&lt;database name&gt;;AuthenticationMethod=type2 as the connection URL, and com.mercury.jdbc.sqlserver.SQLServerDriver as your database driver. Leave the <b>Database User Name</b> and <b>Database Password</b> boxes empty so that the credentials of the currently logged on Windows user (the account from which SiteScope service is running) are used to establish a connection to the database.</p>
<b>Database driver</b>	<p>Enter the JDBC or ODBC driver that SiteScope should use. The .jar file or library containing the .class file must be installed in the &lt;SiteScope root directory&gt;\java\lib\ext directory. To use a database other than jdbc:odbc:orders, you must install the driver files into the proper directory before SiteScope can use them.</p> <p><b>Default value:</b> sun.jdbc.odbc.JdbcOdbcDriver</p>

GUI Element	Description
<b>Credentials</b>	<p>If the database specified requires a name and password for access, select the option to use for authorizing credentials:</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the database in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password for the database (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>Query</b>	(Optional) Enter a SQL query to run on the database. If you do not supply a SQL query string, the driver is loaded and the connection to the database is tested but no query is run.
<b>Result set maximum columns</b>	<p>If you have entered a SQL Query, enter the maximum number of columns to display in the query result set.</p> <p><b>Default value: 10</b></p>
<b>Result set maximum rows</b>	<p>If you have entered a SQL Query, enter the maximum number of rows to display in the query result set.</p> <p><b>Default value: 10</b></p>
<b>Run Tool</b>	Click to run the connection test. Connection results are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.



The following is an example of the data returned from a successful database connection with a SQL query (limited to one row).

server Name	group ID	frame Index	frame ID	setting Name	setting Line	line Chunk	chunk Value
10.0.0.157	master.config	1	_config	_database Max Summary	1	1	200

## Database Information Tool


<b>Description</b>	<p>The Database Information diagnostic tool is used to display database server metadata such as product and driver version, SQL compatibility level information, and supported SQL functions.</p> <p><b>To access:</b> Select <b>Tools</b> context &gt; <b>Database Tools</b> &gt; <b>Database Information Tool</b> (you must have <b>Use tools</b> permissions)</p>
<b>Important Information</b>	Different database drivers and user names can significantly change what information is displayed.
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The Database Information Tool includes the following elements:

GUI Element	Description
<b>Database connection URL</b>	<p>Enter the correct Database connection URL used when setting up the monitor. When using the Oracle thin driver, the database connection URL has the form of: jdbc:oracle:thin:@&lt;server name or IP address&gt;:&lt;port&gt;:&lt;database sid&gt;.</p> <p><b>Example:</b> To connect to the ORCL database on a machine using port 1521, enter jdbc:oracle:thin:@206.168.191.19:1521:ORCL. The colon (:) and the (@) symbols must be included as shown.</p>
<b>Database driver</b>	<p>Enter the JDBC or ODBC driver that SiteScope should use. The .jar file or library containing the .class file must be installed in the &lt;SiteScope root directory&gt;\java\lib\ext directory. To use a database other than jdbc:odbc:orders, you must install the driver files into the proper directory before SiteScope can use them.</p> <p><b>Default value:</b> sun.jdbc.odbc.JdbcOdbcDriver</p>
<b>Credentials</b>	<p>If the database specified requires a name and password for access, select the option to use for authorizing credentials:</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the database in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password for the database (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>

GUI Element	Description
<b>Run Tool</b>	Click to display database information. Test results are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## DNS Lookup Tool


<b>Description</b>	<p>Looks up names from a Domain Name Server and shows you the IP address for a domain name. It also shows you information about the name servers for a domain.</p> <p>You can use this utility to verify that your DNS server is returning the correct addresses for your own servers. You can also use it to verify that it is able to look up the addresses for external domains.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>Network Tools</b> &gt; <b>DNS Lookup Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ The tool is also available when configuring or viewing the DNS monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions): <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
--------------------	---

<b>Included in Tasks</b>	“Use a Tool When Configuring or Editing a Monitor” on page 195
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The DNS Settings panel includes the following elements:

<b>GUI Element</b>	<b>Description</b>
<b>DNS server</b>	Enter the IP address or host name of a DNS server. If left empty, the local DNS server is used.
<b>Host name to resolve</b>	Enter the domain name that you want translated into an IP address.
<b>Run Tool</b>	Click to initiate the test. The tool sends the request to the DNS server entered in the <b>DNS server</b> box and displays the IP address for the host name entered in the <b>Host name to resolve</b> box. The results of the test are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

 **Event Log Tool**


<b>Description</b>	<p>Displays portions of the Windows event log locally or on a remote server.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>Operating System Tools</b> &gt; <b>Event Log Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the Microsoft Windows Event Log monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Different database drivers and user names can significantly change what information is displayed.</li> <li>▶ This tool is not supported on SiteScopes installed on UNIX platforms.</li> </ul>
<b>Included in Tasks</b>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Tools Overview” on page 193</li> <li>▶ “Tools Menu” on page 97</li> </ul>

The Event Log Tool includes the following elements:

GUI Element	Description
<b>Server</b>	<p>The server on which you want to monitor event logs. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. A double slash ("\\") is automatically prefixed to any machine name supplied in the <b>Enter server name</b> box.</li> </ul> <p><b>Note:</b> You must have domain privileges or authenticated access to the Windows remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>

GUI Element	Description
<b>Log name</b>	Select the type of log file you want to view: <ul style="list-style-type: none"> <li>➤ Application</li> <li>➤ Directory Service</li> <li>➤ DNS</li> <li>➤ File Replication Service</li> <li>➤ Security</li> <li>➤ System</li> </ul> <b>Default value:</b> System
<b>Number of events displayed</b>	The number of entries to list for this event log. The most recent entries in the log are displayed first. <b>Default value:</b> 10
<b>Run Tool</b>	Click to initiate the test and refresh the log entry listing. Log entries are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## FTP Server Tool

<b>Description</b>	<p>Use to access an FTP server and view the interaction between SiteScope (acting as an FTP client) and the FTP server. For example, if you receive an alert from SiteScope indicating that your FTP server is not working properly, the first step is to use this tool to help track down the problem.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>➤ Select <b>Tools</b> context &gt; <b>Web Tools</b> &gt; <b>FTP Server Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>➤ This tool is also available when configuring or viewing the FTP monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>➤ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>➤ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<b>Included in Tasks</b>	“Use a Tool When Configuring or Editing a Monitor” on page 195
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The FTP Settings panel includes the following elements:

GUI Element	Description
<b>Basic HTTP Settings</b>	
<b>FTP server</b>	<p>Enter the IP address or the name of the FTP server that you want to test.</p> <p><b>Example:</b> 206.168.191.22 or ftp.thiscompany.com</p>




GUI Element	Description
<b>File</b>	Enter the file name to retrieve. <b>Example:</b> /pub/docs/mydoc.txt
<b>User name</b>	Enter the name used to log on to the FTP server.
<b>Password</b>	Enter the password used to log on to the FTP server.
<b>Passive mode</b>	Select to have SiteScope use a passive FTP connection. This is commonly required to access FTP servers through a firewall.
<b>HTTP Proxy Settings</b>	
<b>HTTP proxy</b>	Enter the proxy name or IP address if you want to use a proxy server for the FTP test.
<b>Proxy user name</b>	Enter the name used to log into the proxy server.
<b>Proxy password</b>	Enter the password used to log into the proxy server.
<b>Run Tool</b>	Click to initiate the test. Check The results of the test are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

The following is a sample output from the Check FTP Server tool. In this case, the FTP server allowed us to log on without a problem, indicating that the server is running and accepting requests. The failure is caused when the server was unable to locate the file that was requested: file.txt. Correcting this particular problem may be as easy as replacing the missing file or verifying the file location.

```
Received: 220 public Microsoft FTP Service (Version 2.0).  
Sent: USER anonymous  
Received: 331 Anonymous access allowed, send identity (e-mail name) as password.  
Sent: PASS anonymous  
Received: 230 Anonymous user logged in.  
Sent: PASV  
Received: 227 Entering Passive Mode (206,168,191,1,5,183).  
Connecting to server 206.168.191.1 port 1463  
Sent: RETR file.txt  
Received: 550 file.txt: The system cannot find the file specified.  
Sent: QUIT  
Received: 221
```

## LDAP Authentication Tool


<p><b>Description</b></p>	<p>Verifies that a Lightweight Directory Access Protocol (LDAP) server can authenticate a user by performing a simple authentication.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>Database Tools</b> &gt; <b>LDAP Authentication Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the LDAP monitor or Active Directory Replication monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “SiteScope Tools Overview” on page 193</li> <li>▶ “Tools Menu” on page 97</li> </ul>

The LDAP Authentication Tool includes the following elements:

GUI Element	Description
<b>Security principal</b>	<p>Enter the constant that holds the name of the environment property for specifying the identity of the principal that authenticates the caller to the service. The format of the principal depends on the authentication scheme. If this property is unspecified, the behavior is determined by the service provider. This should be in the format: uid=testuser,ou=TEST,o=mydomain.com.</p> <p><b>Note:</b> SiteScope does not support users that contain one or more of the following character inside the users name: equal ("="), semi-colon (";"), inverted commas ("").</p>
<b>Security credential</b>	<p>Enter the constant that holds the name of the environment property for specifying the credentials of the principal for authenticating the caller to the service. The value of the property depends on the authentication scheme. For example, it could be a hashed password, clear-text password, key, certificate, and so on. If this property is unspecified, the behavior is determined by the service provider.</p>
<b>LDAP service provider</b>	<p>Enter the constant that holds the name of the environment property for specifying configuration information for the service provider to use. The value of the property should contain a URL string. This property may be specified in the environment, an applet parameter, a system property, or a resource file. If it is not specified in any of these sources, the default configuration is determined by the service provider.</p> <p><b>Example:</b> ldap://&lt;somehost&gt;:389</p>
<b>Object query</b>	<p>Use this box to enter an object query to look at a LDAP object other than the default user <b>dn</b> object. You must enter a valid object query in this text box if you are using a LDAP filter. For details about the search filter, see the description below.</p> <p><b>Example:</b> Enter the mail object to check for an email address associated with the <b>dn</b> object entered above.</p>

GUI Element	Description
<b>LDAP filter</b>	<p>Enter a search filter in this text box to perform a search using a filter criteria. The LDAP filter syntax is a logical expression in prefix notation meaning that logical operator appears before its arguments.</p> <p><b>Example:</b> The item <code>sn=Freddie</code> means that the <code>sn</code> attribute must exist with the attribute value equal to Freddie.</p> <p>Multiple items can be included in the filter string by enclosing them in parentheses, such as <code>(sn=Freddie)</code> and combined using logical operators such as the <code>&amp;</code> (the conjunction operator) to create logical expressions.</p> <p><b>Example:</b> The filter syntax <code>(&amp; (sn=Freddie) (mail=*))</code> requests LDAP entries that have both a <code>sn</code> attribute of Freddie and a <code>mail</code> attribute.</p>
<b>Run Tool</b>	Click to initiate the test. LDAP Authentication test results are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## Mail Round Trip Tool

<p><b>Description</b></p>	<p>Checks a Mail Server by using the network and verifies that the mail server is accepting requests and that a message can be sent and retrieved. It does this by sending a standard mail message using SMTP and then retrieving that same message by using a POP user account. Each message that SiteScope sends includes a unique key which it checks for to insure that it does not retrieve the wrong message and return a false OK reading.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>➤ Select <b>Tools</b> context &gt; <b>Mail Tools</b> &gt; <b>Mail Round Trip Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>➤ This tool is also available when configuring or viewing the Mail monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>➤ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>➤ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The Mail Round Trip Tool includes the following elements:


GUI Element	Description
<b>Basic Mail Settings</b>	
<b>Action</b>	Select the action to take: <ul style="list-style-type: none"> <li>▶ <b>Send and receive.</b> Allows you to send a test message to an SMTP server and then receive it back from the POP3 or IMAP4 server to check that the mail server is up and running. (Default option)</li> <li>▶ <b>Receive only.</b> Checks the incoming POP3 or IMAP4 mail servers for a message that was sent previously. This check is done by matching the content of the previously-sent message.</li> <li>▶ <b>Send only.</b> Checks that the receiving mail server has accepted the message.</li> </ul>
<b>Sending email server (SMTP)</b>	Enter the host name of the SMTP mail server to which the test mail message should be sent. <b>Example:</b> mail.thiscompany.com
<b>Send to address</b>	Enter the mail address to which the test message should be sent.
<b>Receiving protocol</b>	Select the protocol used by the receiving mail server. Use the POP3 option to check the POP3 mail server for a sent message. Use the IMAP4 option to check the IMAP mail server for a sent message. <b>Default value:</b> POP3
<b>Receiving email server</b>	Enter the host name of the POP mail server that should receive the test message. This can be the same mail server to which the test message was sent. <b>Example:</b> mail.thiscompany.com

GUI Element	Description
<b>Receiving email server user name</b>	<p>Enter a POP user account name. A test email message is sent to this account and the logs in to the account to verify that the message was received. No other mail in the account is touched. You can use your own personal mail account or another existing account for this purpose.</p> <p><b>Note:</b> If you use an email reader that automatically retrieves and deletes messages from the server, there is a chance that the Mail Round Trip Tool never sees the mail message and reports an error.</p>
<b>Receiving email server password</b>	<p>Enter a password, if necessary, for the test mail account.</p>
<b>Receive only content match</b>	<p>Enter a string of text to match against the contents of the incoming message. If the text is not contained in the incoming message, the Mail Round Trip reports an error. This is for the receiving only option (for example, Subject:MySubject). The search is case sensitive.</p> <p>HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, "&lt; B&gt; Hello&lt; /B&gt; World"). This works for XML pages as well.</p> <p>You can perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching. An example might be <code>"/href=Doc\d+\.\html/"</code> or <code>"/href=doc\d+\.\html/i"</code>.</p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a regular expression (for example, <code>/Temperature: (d+)/</code>). This returns the temperature as it appears on the page.</p>



GUI Element	Description
<b>Advanced Mail Settings</b>	
<b>Timeout (seconds)</b>	The number of seconds to wait for a mail message to be received before timing-out. <b>Default value:</b> 300 seconds
<b>POP check delay (seconds)</b>	After SiteScope sends the test message, it immediately logs into the mail account to verify that the message has been received. If the message has not been received, SiteScope automatically waits 10 seconds before it checks again. You can adjust this wait time by indicating an alternate number of seconds to wait in this box. <b>Default value:</b> 10 seconds
<b>NTLM authentication</b>	If NTLM authentication is used by the email server, select the NTLM version (version 1 or 2). <b>Default value:</b> none
<b>Show details</b>	Select this box if you want details of the round trip test to be displayed
<b>Run Tool</b>	Click to initiate the test. Check mail server test results are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## Microsoft Windows Media Player Tool

<b>Description</b>	<p>Use this tool for testing Microsoft Windows Media Player streaming.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>➤ Select <b>Tools</b> context &gt; <b>Application Tools</b> &gt; <b>Microsoft Windows Media Player Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>➤ This tool is also available when configuring or viewing the Microsoft Windows Media Player monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>➤ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>➤ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<b>Included in Tasks</b>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The Microsoft Windows Media Player Tool includes the following elements:

GUI Element	Description
<b>URL</b>	<p>Enter the URL of the media file or streaming source you want to test. This should be the URL of the media file.</p> <p><b>Example:</b> mms://&lt;servername&gt;/sample.asf for a unicast stream or http://&lt;servername&gt;/stationid.nsc for a multicast stream using a Windows Media Server multicast station program.</p> <p><b>Note:</b> This monitor does not support the .asx or .mov formats.</p>
<b>Duration (milliseconds)</b>	<p>Enter the playback duration that the tool should use for the media file or source. The duration value does not need to match the duration of the media contained in the file.</p> <p>If the media content of the file or source you are testing is less than the duration value selected for the test, the monitor plays the entire media content and reports the results, including the time required to play the media content.</p>
<b>Run Tool</b>	<p>Click to initiate the test. Check mail server test results are displayed in the Results panel.</p>
<b>Save to File</b>	<p>Click to open the Save dialog box and save the results to a file.</p>


## Network Status Tool

<b>Description</b>	<p>The Network Status Tool reports the current network interface statistics and lists the active network connections. This information can be useful to determine the health of your network interface. You can also use this tool to track down problems where network connections are being left open or runaway conditions where an increasing number of connections are being opened without being closed.</p> <p><b>To access:</b> Select <b>Tools</b> context &gt; <b>Network Tools</b> &gt; <b>Network Status Tool</b> (you must have <b>Use tools</b> permissions)</p>
<b>Important Information</b>	This tool is not supported on SiteScopes installed on UNIX platforms.
<b>Included in Tasks</b>	“Use a Tool When Configuring or Editing a Monitor” on page 195
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The Network Status Settings panel includes the following elements:

GUI Element	Description
<b>Run Tool</b>	Click to run the Network Status Tool and report the network information. The data is displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## News Server Tool


<b>Description</b>	<p>You can use the Check News Server as a tool to access a News server and view the NNTP interaction between SiteScope (acting as a news client) and the News server.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>Application Tools</b> &gt; <b>News Server Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the News monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<b>Included in Tasks</b>	“Use a Tool When Configuring or Editing a Monitor” on page 195
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Tools Overview” on page 193</li> <li>▶ “Tools Menu” on page 97</li> </ul>

The News Server Tool includes the following elements:

GUI Element	Description
<b>News server</b>	Enter the name of the News server in the format news.sitescope.com or news.sitescope.com:7777.
<b>News groups</b>	(Optional) Enter one or more news groups. Separate multiple news group names by commas (",").
<b>User name</b>	If the News server specified above requires a name and password for access, enter the user name.

GUI Element	Description
<b>Password</b>	If the News server specified above requires a name and password for access, enter the password.
<b>Run Tool</b>	Click to initiate the test. The results of the test are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## Performance Counters Tool

<p><b>Description</b></p>	<p>The Performance Counter Test is a tool that you can use to check performance counters on a specific machine in a Windows NT/2000 network. It provides an interface to the <b>perfex.exe</b> executable supplied as part of SiteScope.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>Operating System Tools</b> &gt; <b>Performance Counters Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the CPU monitor, Disk Space monitor, Memory monitor, or Microsoft Windows Performance Counter monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<p><b>Important Information</b></p>	<p>This tool is not supported on SiteScopes installed on UNIX platforms.</p>
<p><b>Included in Tasks</b></p>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “SiteScope Tools Overview” on page 193</li> <li>▶ “Tools Menu” on page 97</li> </ul>

The Performance Counters Tool includes the following elements:


GUI Element	Description
<b>Server</b>	<p>The server where the Windows performance counter objects you want to monitor are running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. A double slash ("\\") is automatically prefixed to any machine name supplied in the <b>Enter server name</b> box.</li> </ul> <p><b>Note:</b> You must have domain privileges or authenticated access to the Windows remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>



GUI Element	Description
<b>Counters</b>	Select a counter object to display the individual performance counters and corresponding values for the selected counter object.
<b>Run Tool</b>	Click to display the individual Windows performance counters and corresponding values for the selected counter object. This information is displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.



## Ping Tool

<p><b>Description</b></p>	<p>Ping is a tool that sends a packet to another location and back to the sender. It shows you the round trip time along the path. When there is a problem with the network, ping can tell you if another location can be reached. The Ping tool does a ping from the current server to another location.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>➤ Select <b>Tools</b> context &gt; <b>Network Tools</b> &gt; <b>Ping Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>➤ This tool is also available when configuring or viewing the Ping monitor or Port monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>➤ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>➤ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The Ping Settings panel includes the following elements:

GUI Element	Description
<b>Host name to resolve</b>	Enter the domain name or IP address of the host you want to ping. <b>Example:</b> demo.thiscompany.com or 206.168.112.53
<b>Run Tool</b>	Click to ping the domain name or IP address. The results of the test are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## **Processes Tool**


<b>Description</b>	<p>The Processes tool displays processes running on the server where SiteScope is installed. This can be useful to confirm that critical processes are available.</p> <p><b>To access:</b> Select <b>Tools</b> context &gt; <b>Operating System Tools</b> &gt; <b>Processes Tool</b> (you must have <b>Use tools</b> permissions)</p>
<b>Included in Tasks</b>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Tools Overview” on page 193</li> <li>▶ “Tools Menu” on page 97</li> </ul>

The Processes Tool includes the following elements:

GUI Element	Description
<b>Server</b>	<p>The server where the processes you want to monitor are running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. A double slash ("\\") is automatically prefixed to any machine name supplied in the <b>Enter server name</b> box.</li> </ul> <p><b>Note:</b> You must have domain privileges or authenticated access to the Windows remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>

GUI Element	Description
<b>Run Tool</b>	Click to initiate the test. The results of the test are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## Real Media Player Tool

<b>Description</b>	<p>Use this tool for testing Real Media Player streaming.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>Application Tools</b> &gt; <b>Real Media Player Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the Real Media Player monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions): <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<b>Included in Tasks</b>	“Use a Tool When Configuring or Editing a Monitor” on page 195
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Tools Overview” on page 193</li> <li>▶ “Tools Menu” on page 97</li> </ul>

The Real Media Player Tool includes the following elements:

GUI Element	Description
<b>URL</b>	<p>Enter the URL of the media file or streaming source you want to test. This should be the URL of the media file.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ You can test video streams only (not audio) with this tool.</li> <li>▶ This tool does not support metadata files such as the .smi format.</li> </ul>
<b>Duration (milliseconds)</b>	<p>Enter the playback duration that the tool should use for the media file or source. The duration value does not need to match the duration of the media contained in the file.</p> <p>If the media content of the file or source you are testing is less than the duration value selected for the test, the monitor plays the entire media content and reports the results, including the time required to play the media content.</p>
<b>Run Tool</b>	<p>Click to initiate the test. The results of the test are displayed in the Results panel.</p>
<b>Save to File</b>	<p>Click to open the Save dialog box and save the results to a file.</p>

## Regular Expression Tool

<b>Description</b>	Enables you to perform a regular expression match. <b>To access:</b> Select <b>Tools</b> context > <b>Common Utility Tools</b> > <b>Regular Expression Tool</b> (you must have <b>Use tools</b> permissions)
<b>Included in Tasks</b>	“Use a Tool When Configuring or Editing a Monitor” on page 195
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Tools Overview” on page 193</li> <li>▶ “Tools Menu” on page 97</li> </ul>

The Regular Expression Tool includes the following elements:

GUI Element	Description
<b>Text</b>	Copy and paste a portion of text containing the string or values on which you want to perform a regular expression match into this box.  For efficiency in developing regular expressions, you should include all of the content that would precede the target data or pattern that you want to match. For example, when developing a regular expression for content matching on a Web page, you should use the URL Tool to retrieve the entire HTTP content including the HTTP header.
<b>Regular expression</b>	Enter a regular expression between the slashes //, to match some part of the text you entered.  <b>Note:</b> For content with multiple lines with carriage returns and line feeds, consider adding the s search modifier to the end of the expression to have the content treated as a single line of text.  <b>Example:</b> /value:\W[\d]{2,6}/s



GUI Element	Description
<b>Run Tool</b>	Click to perform the test. The results of the match test are displayed in the Results panel. If there is a problem with your regular expression, an error message is displayed.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.


### **Parsed Parentheses and Matches Table**

This section includes a table that displays any matches requested as retained values or back references by pairs of parentheses inside the regular expression. If your expression does not include parentheses, this table is empty. The columns of the parsed parentheses table are:

GUI Element	Description
<b>Parentheses counted from left</b>	Displays any patterns in the regular expression delimited by parentheses as counted from the left-hand side of the expression.
<b>Matching text</b>	Displays the text that matched the parenthesis marked patterns listed in the column to the left.
<b>Whole Match Between Slashes</b>	This is the text area below the table. It echoes the entire content entered in the <b>Your Text that will be matched</b> box. The content that matched the pattern in your regular expression is highlighted within this content, normally using a blue font. This is useful for showing possible problems with wildcard expressions like the <code>.*</code> pattern that match too much content. It can also uncover problems of duplicate patterns within the content that require you to add other unique patterns to your expression to match the desired portion of the content.



## Services Tool


<b>Description</b>	<p>Displays services running on the server where SiteScope is installed. This can be useful to confirm that critical services are available. If Remote UNIX machines have been defined, they are listed in a drop-down menu.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>Operating System Tools</b> &gt; <b>Services Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the Service monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<b>Important Information</b>	This tool is not supported on SiteScopes installed on UNIX platforms.
<b>Included in Tasks</b>	“Use a Tool When Configuring or Editing a Monitor” on page 195
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Tools Overview” on page 193</li> <li>▶ “Tools Menu” on page 97</li> </ul>

The Services Tool includes the following elements:

GUI Element	Description
<b>Server</b>	<p>The server where the services you want to monitor are running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. A double slash ("\\") is automatically prefixed to any machine name supplied in the <b>Enter server name</b> box.</li> </ul> <p><b>Note:</b> You must have domain privileges or authenticated access to the Windows remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>

GUI Element	Description
<b>Run Tool</b>	Click to initiate the test. The results of the test are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## SNMP Browser Tool

<p><b>Description</b></p>	<p>The SNMP Browser Tool provides an XML representation of an SNMP agent's MIB. It can be used to verify the connection properties of an SNMP agent and to gain more information about the MIBs which that agent implements.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>SNMP Tools</b> &gt; <b>SNMP Browser Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the Cisco Works monitor, F5 Big-IP monitor, or SNMP by MIB monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This tool operates by traversing all of the OIDs on a given agent and then using the MIB information in the <b>&lt;SiteScope root directory&gt;\templates.mib</b> directory to build an XML representation of the OIDs. Included in the XML tree are the textual and numeric names of the OIDs, their descriptions (if available), and their values at the time of traversal.</li> <li>▶ The XML is displayed in a separate Results panel that displays lines numbers and highlights specific XML. If errors occur during the MIB traversal, an error message describing the problem is printed in the Results panel.</li> </ul>

<b>Included in Tasks</b>	“Use a Tool When Configuring or Editing a Monitor” on page 195
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The SNMP Browser Tool includes the following elements:


GUI Element	Description
<b>SNMP Connection Settings</b>	
<b>Server</b>	Enter the host name or IP address of the device on which the SNMP agent is running that you want to monitor.
<b>SNMP version</b>	Select the version of SNMP which the tool should use when connecting to the agent. <b>Default value:</b> V1
<b>Community</b>	For version 1 or 2 connections, enter the community string to use when connecting to the SNMP agent. <b>Default value:</b> public
<b>Timeout (seconds)</b>	Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. <b>Default value:</b> 5 seconds
<b>Retries</b>	Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. <b>Default value:</b> 1
<b>Port</b>	Enter the port on which the SNMP agent is listening. <b>Default value:</b> 161

GUI Element	Description
<b>Starting OID</b>	Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered here. The default value is 1, which is commonly used and applicable to most applications. You should edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value of 1 did not enable retrieving any counters, then you may have to enter a different value.
<b>MIB file</b>	Choose the MIB that you want to view. If you select <b>All MIBs</b> , then all data obtained during the MIB traversal is displayed. If you select a specific MIB, then only the OIDs within that MIB are displayed. This list of MIBs can be updated or extended by placing new MIB files in the <b>&lt;SiteScope root directory&gt;\templates.mib</b> directory. <b>Default value:</b> All MIBs
<b>Counter calculation mode</b>	Select a counter calculation mode option: <ul style="list-style-type: none"> <li>➤ <b>Calculate delta.</b></li> <li>➤ <b>Calculate rate.</b></li> <li>➤ <b>Do not calculate.</b></li> </ul>
<b>V3 SNMP Settings</b> (This panel is enabled only if V3 is selected in the SNMP version field)	
<b>SNMP V3 authentication type</b>	Select the type of authentication to use for a version 3 connection. <b>Default value:</b> MD5
<b>SNMP V3 user name</b>	Enter the user name for a version 3 connection.

GUI Element	Description
<b>SNMP V3 authentication password</b>	Enter the password to use for authentication in a version 3 connection.
<b>SNMP V3 privacy password</b>	Enter the password to use for DES privacy encryption in a version 3 connection. Leave this box blank if no privacy is desired.
<b>SNMP V3 context engine ID</b>	Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.
<b>SNMP V3 context name</b>	Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.
<b>Run Tool</b>	Click to initiate the test. The results of the test are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.




 **SNMP Tool**

<b>Description</b>	<p>The SNMP tool lets you query a SNMP Management Information Base (MIB) and retrieve a set of OIDs.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>➤ Select <b>Tools</b> context &gt; <b>SNMP Tools</b> &gt; <b>SNMP Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>➤ This tool is also available when configuring or viewing the SNMP monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>➤ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>➤ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<b>Included in Tasks</b>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The SNMP Tool includes the following elements:

GUI Element	Description
<b>Host name</b>	Enter the IP address of the server that hosts the SNMP MIB you want to query.
<b>Object ID</b>	Enter the ID of the next object that should be retrieved.
<b>Index</b>	<p>Enter the index of the SNMP object. Values for an OID come as either scalar or indexed (array) values. For a scalar OID, the index value must be set to 0. For an indexed value, you must provide the index (a positive integer starting with 1) to the element that contains the value you want.</p> <p><b>Example:</b> OID 1.3.6.1.2.1.2.2.1.17 is an indexed value that contains four elements. To access this second element of this OID, enter an index of 2 in this text box.</p> <p><b>Default value:</b> 0</p>
<b>Community</b>	<p>Enter the Community string for the SNMP device.</p> <p><b>Default value:</b> public</p>
<b>SNMP version</b>	<p>Select the SNMP version used by the SNMP host you want to test. SiteScope supports both SNMP version 1 and version 2.</p> <p><b>Default value:</b> V1</p>
<b>Number of records to get</b>	<p>Enter the number of OID records to retrieve.</p> <p><b>Default value:</b> 1</p>
<b>Run Tool</b>	Click to perform the query. The results of the test are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## SNMP Trap Tool

<b>Description</b>	<p>Lets you view SNMP Traps received by SiteScope's SNMP listener. The tool is only enabled if you have already created one or more SNMP Trap monitors. Creating an SNMP Trap Monitor enables the SiteScope SNMP Trap Log.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>SNMP Tools</b> &gt; <b>SNMP Trap Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the SNMP Trap monitor or Technology SNMP Trap Integration monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<b>Important Information</b>	<p>The message <b>Receiving SNMP Traps is not active</b> is displayed at the top of the tool page if the SNMP Trap Log is not currently active.</p>
<b>Included in Tasks</b>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Tools Overview” on page 193</li> <li>▶ “Tools Menu” on page 97</li> </ul>

The SNMP Trap Tool includes the following elements:

GUI Element	Description
<b>Content match</b>	<p>Enter an optional text string or regular expression to be used to match entries in the SNMP Trap Log. Content matching can be done for data from any of the columns of the log such as OID, Community, Agent, and so on.</p> <p>The SNMP traps in the SiteScope SNMP Trap Log are displayed in the SNMP Trap Log table. The number of traps matching the search criteria are displayed in the SNMP Trap Log table title displayed in the lower part of the page.</p>
<b>Traps to show</b>	<p>Enter the number of SNMP Traps to list. The number of traps is calculated, based on average trap length. If the trap text is longer or shorter than average, the number of traps shown can be different from the selected value. The most recent SNMP Traps received by SiteScope are displayed first.</p> <p><b>Default value: 10</b></p>
<b>Run Tool</b>	<p>Click to view the log based on the search criteria you have entered. The results of the test are displayed in the Results panel.</p>
<b>Save to File</b>	<p>Click to open the Save dialog box and save the results to a file.</p>

 **Trace Route Tool**


<b>Description</b>	<p>Trace Route is a tool that shows you the network path between two locations and how long it takes to get to each hop in the path. When there is a problem with the network, traceroute can often be used to narrow down where the problem is occurring. This tool performs a traceroute from your server to another location.</p> <p>You can use this utility to verify connectivity of a host and to determine how the host is connected to the Internet. You can also determine the path taken from your server to the specified host. This helps you to determine where packet loss may be occurring when you attempt to connect to hosts elsewhere on the Internet.</p> <p><b>To access:</b> Select <b>Tools</b> context &gt; <b>Network Tools</b> &gt; <b>Trace Route Tool</b> (you must have <b>Use tools</b> permissions)</p>
<b>Important Information</b>	<p>You can use this tool to perform a traceroute on Windows platforms only. For UNIX, you must stop the SiteScope process, add the path of the traceroute utility (for example <code>/usr/sbin/traceroute</code>) to the <b>Traceroute command</b> box in Infrastructure Settings Preferences, and then restart SiteScope.</p>
<b>Included in Tasks</b>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The Trace Route Tool includes the following elements:

GUI Element	Description
<b>Host name to resolve</b>	Enter the domain name or IP address of the other location to resolve. <b>Example:</b> demo.thiscompany.com or 206.168.112.53
<b>Run Tool</b>	Click to initiate the action. The results of the test are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.



## URL Tool

<b>Description</b>	<p>Use to retrieve an item from a Web server. The URL specifies the server to contact and the item to return. Because SiteScope displays the content of the requested URL, this tool also functions to check URL Content. You can use this utility to verify that a given URL can be accessed from a Web server. You can also use it to see how long it takes for the page to be returned.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>Web Tools</b> &gt; <b>URL Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the URL monitor, URL Content monitor, or Oracle 9i Application Server monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<b>Included in Tasks</b>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Tools Overview” on page 193</li> <li>▶ “Tools Menu” on page 97</li> </ul>

The URL Tool includes the following elements:


GUI Element	Description
<b>Main Settings</b>	
<b>URL</b>	Enter the URL that you want to test. <b>Example:</b> http://demo.company.com
<b>Match content</b>	Enter a string of text to check for in the returned page or frame set. If the text is not contained in the page, the content match fails. The search is case sensitive. HTML tags are part of a text document, so you must include the HTML tags if they are part of the text you are searching for (for example, "< B> Hello< /B> World").
<b>Match content for error</b>	Enter a string of text to check for in the returned page or frame set. If the text is contained in the page, the test indicates an error condition. The search is case sensitive.
<b>HTTP Settings</b>	
<b>URL content encoding</b>	<p>URL content encoding is the encoding in which the content is written. The encoding can be found in any of the following:</p> <ul style="list-style-type: none"> <li>▶ HTTP headers: Content-Type: text/html; charset=UTF-8</li> <li>▶ HTML meta tag &lt;meta http-equiv="Content-Type" content="text/html; charset=US-ASCII"&gt;</li> <li>▶ XML: &lt;?xml version="1.0" encoding="ISO-8859-1"?&gt;</li> </ul> <p>Select the encoding type from the drop down list.</p> <p><b>Examples:</b> UTF-8, UTF-16, US-ASCII, ISO-8859-1</p> <p><b>Default value:</b> Encoding from server response</p>
<b>Retrieve images</b>	Select this option to have SiteScope list the images such as graphics, logos, and so on linked to the URL being requested.
<b>Retrieve frames</b>	Select this option to have SiteScope display the HTML code of a frame linked to the URL being requested.



GUI Element	Description
<b>Authentication Settings</b>	
<b>Credentials</b>	<p>If the URL specified requires a name and password for access, select the option to use for authorizing credentials:</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the URL in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password for the URL (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>NTLM V2</b>	Check this parameter if you want to use NTLM (Windows NT LAN Manager) version 2 to authenticate user logon.
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	Optionally, a proxy server can be used to access the URL. Enter the address or domain name and port of an HTTP Proxy Server.
<b>Proxy server user name</b>	Enter the name used to log on to the proxy server.
<b>Proxy server password</b>	Enter the password used to log on to the proxy server.

GUI Element	Description
<b>Proxy NTLM V2</b>	Check this parameter if the proxy uses NTLM (Windows NT LAN Manager) version 2 to authenticate user logon.
<b>Run Tool</b>	Click to initiate the test. The results of the test are displayed in the Results panel. The results include statistics on the URL retrieval as well as a text representation of the URL content.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.

## Web Service Tool

<p><b>Description</b></p>	<p>Checks Simple Object Access Protocol (SOAP) enabled Web services for availability, stability, or to see what an actual SOAP response looks like. It is also useful for diagnosing a Web service request failure, or for picking out match strings for use with a specific Web Service Monitor. The Web Service Test sends a SOAP request to the server and checks the HTTP response codes to verify that the service is responding. The actual SOAP response is displayed, but no further verification is done on this returned message.</p> <p>SOAP is a way for a program running under one operating system to communicate with another program running under the same or different operating system (such as a Windows 2000 program talking to a Linux-based program). SOAP uses the Hypertext Transfer Protocol (HTTP) and Extensible Markup Language (XML) for information exchange with services in a distributed environment.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>▶ Select <b>Tools</b> context &gt; <b>Web Tools</b> &gt; <b>Web Service Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>▶ This tool is also available when configuring or viewing the Web Service monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>▶ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>▶ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
---------------------------	--

<b>Important Information</b>	<ul style="list-style-type: none"> <li>➤ The following specification features are currently supported: WSDL 1.2, SOAP 1.1, Simple and Complex Types based on XML Schema 2001, SOAP binding with the HTTP(s) protocol only. SOAP with Attachments is not supported.</li> <li>➤ SOAP and WSDL technologies are evolving. As a result, some WSDL documents may not parse accurately and some SOAP requests may not interact with all Web service providers.</li> </ul>
<b>Included in Tasks</b>	"Use a Tool When Configuring or Editing a Monitor" on page 195
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ "SiteScope Tools Overview" on page 193</li> <li>➤ "Tools Menu" on page 97</li> </ul>

The Web Service Tool includes the following elements:

GUI Element	Description
<b>WSDL Settings</b>	
<b>WSDL location</b>	Select the WSDL location: <ul style="list-style-type: none"> <li>➤ <b>File.</b> Select the WSDL file to be used. This list reflects the files found by searching on &lt;SiteScope root directory&gt;\templates.wSDL/*.wSDL. Your WSDL files must have an extension of .wSDL.</li> <li>➤ <b>URL.</b> Enter the URL of the Web service to be tested.</li> </ul>
<b>Get Data</b>	Clicking the <b>Get Data</b> button causes the specified WSDL file to be retrieved and analyzed for method arguments. The ensuing page displays the measurements available.
<b>Service name</b>	Select the name of the service to be invoked. During initial setup, this is extracted from the WSDL file.
<b>Port name</b>	Select the name of the port to be invoked. During initial setup, this is extracted from the WSDL file.
<b>Method name</b>	Select the name of the method to be invoked. During initial setup, this is extracted from the WSDL file.

GUI Element	Description
<b>Method name space</b>	The XML name space for the method in the SOAP request. During initial setup this value is extracted from the WSDL file.
<b>Schema name space</b>	The XML name space for the schema in the SOAP request. During initial setup, this value is extracted from the WSDL file.
<b>SOAP action</b>	The SOAP action URL in the header of the SOAP request to the Web Service. During initial setup, this is extracted from the WSDL file.

GUI Element	Description
<p><b>Name of arguments</b></p>	<p>Enter the arguments to the method specified above and their types. Specify simple type parameters in the format <code>parm-name(parm-type) = value</code>, where the <code>&lt;param-name&gt;</code> and <code>&lt;param-type&gt;</code> must match the service method specifications of its WSDL file exactly. The <code>&lt;value&gt;</code> must agree with the <code>&lt;param-type&gt;</code>, otherwise the request fails. Strings with embedded spaces should be enclosed in double quotes (" "). Each parameter must be on a separate line by adding a carriage return at the end of each value.</p> <p><b>Example:</b> <code>stockSymbol (string) = MERQ</code>  <code>numShares (int) = 10</code></p> <p>A complex type parameter must be represented as one long string (line breaks are for readability purposes only):</p> <pre>stocksymbol[COMPLEX] = &lt;stocksymbol xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fw100="urn:ws-stock" xsi:type="fw100:getQuote"&gt; &lt;ticker xsi:type="xsd:string"&gt;MERQ &lt;/ticker&gt; &lt;/stocksymbol&gt;</pre> <p><b>Note:</b> SiteScope does not perform any validation on your input parameter lists, so make sure that the complex type values are valid and well-formed XML strings. Do not add any carriage returns within a complex type parameter—only at the end.</p> <p>If the Web service method does not take any parameters, the text box should be left empty.</p>
<p><b>Use user-defined SOAP XML</b></p>	<p>Select this check box to use the XML in the <b>Use SOAP XML</b> box. This enables you to use XML that has been manually defined.</p>


GUI Element	Description
<b>Use SOAP XML</b>	Displays the SOAP XML for the selected Web service extracted from the WSDL file. You can make changes to the default XML, and use the manually defined XML in this box by selecting the <b>Use User-Defined SOAP XML</b> check box.
<b>Main Settings</b>	
<b>Request's schema</b>	The request schema. Currently SiteScope only supports SOAP.
<b>Timeout (seconds)</b>	Enter the total time, in seconds, that SiteScope should wait for the Web service request to complete. <b>Default value:</b> 30 seconds
<b>Use .NET SOAP</b>	Select this check box if the Web service is based on Microsoft .NET.
<b>Content match</b>	<p>Enter a string of text to check for in the returned page or frameset. If the text is not contained in the page, the tool displays the message no match on content.</p> <p>HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for. This works for XML pages as well.</p> <p><b>Example:</b> "&lt; B&gt; Hello&lt; /B&gt; World"</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash to indicate that the search is not case sensitive.</p> <p><b>Example:</b> <code>/href=Doc\d+\.html/</code> or <code>/href=doc\d+\.html/i</code></p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression.</p> <p><b>Example:</b> <code>/Temperature: (\d+)</code></p> <p><b>Note:</b> The search is case sensitive.</p>

GUI Element	Description
<b>HTTP Settings</b>	
<b>Web service server URL</b>	Shows the URL of the Web service server to be checked.
<b>HTTP user agent</b>	The HTTP user agent for the SOAP request.
<b>HTTP content type</b>	The content type of the HTTP request.
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	(Optional) A proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.
<b>Proxy server user name</b>	If the proxy server requires a name and password to access the URL, enter the password here. <b>Note:</b> Your proxy server must support Proxy-Authentication for these options to function.
<b>Proxy server password</b>	If the proxy server requires a name and password to access the URL, enter the password here. <b>Note:</b> Your proxy server must support Proxy-Authentication for these options to function.
<b>Login Settings</b>	
<b>NTLM domain</b>	If the Web service requires NTLM / Challenge Response authentication, a domain name is required as part of your credentials (as well as a user name and password below).
<b>Authorization user name</b>	If the Web service requires a user name and password for access (Basic, Digest, or NTLM authentication), enter the user name.  Alternately, you can leave this entry blank and enter the user name in the <b>Default authentication user name</b> box on the General Preferences page. You use this alternate method to define common authentication credentials.



GUI Element	Description
<b>Authorization password</b>	<p>If the Web service requires a user name and password for access (Basic, Digest or NTLM authentication), type the password.</p> <p>Alternately, you can leave this entry blank and enter the password in the <b>Default authentication password</b> box on the General Preferences page. You use this alternate method to define common authentication credentials.</p>
<b>Run Tool</b>	<p>Click to test the Web Service request. The results of the test are displayed in the Results panel.</p> <p>The possible status values returned by the test are:</p> <ul style="list-style-type: none"> <li>➤ OK</li> <li>➤ unknown host name</li> <li>➤ unable to reach server</li> <li>➤ unable to connect to server</li> <li>➤ timed out reading</li> <li>➤ content match error</li> <li>➤ document moved</li> <li>➤ unauthorized</li> <li>➤ forbidden</li> <li>➤ not found</li> <li>➤ proxy authentication required</li> <li>➤ server error</li> <li>➤ not implemented</li> <li>➤ server busy</li> </ul>
<b>Save to File</b>	<p>Click to open the Save dialog box and save the results to a file.</p>

## XSL Transformation Tool

<p><b>Description</b></p>	<p>Use this tool to test a user-defined XSL file that can be used to transform an XML file or output. This might be a file from a Web application that contains performance metrics data. The use of an XSL transformation may be necessary to process XML data into an acceptable format for use by the browsable XML Monitor.</p> <p><b>To access:</b></p> <ul style="list-style-type: none"> <li>➤ Select <b>Tools</b> context &gt; <b>Common Utility Tools</b> &gt; <b>XSL Transformation Tool</b> (you must have <b>Use tools</b> permissions).</li> <li>➤ This tool is also available when configuring or viewing the XML Metrics monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions):             <ul style="list-style-type: none"> <li>➤ Click the <b>Use Tool</b> button in the new monitor dialog box when configuring a new monitor, or in the monitor <b>Properties</b> tab when configuring an existing monitor.</li> <li>➤ To run the test tool for an existing monitor, click the <b>Tools</b>  button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results panel.</li> </ul> </li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Use a Tool When Configuring or Editing a Monitor” on page 195</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ “SiteScope Tools Overview” on page 193</li> <li>➤ “Tools Menu” on page 97</li> </ul>

The XML Transformation Tool includes the following elements:

GUI Element	Description
<b>Main Settings</b>	
<b>XML URL</b>	Enter the URL of the XML file that is the input for the transformation.
<b>XSL file</b>	Enter the path to the XSL file you want to test. This path must be relative to SiteScope root folder. <b>Example:</b> <SiteScope root directory>\templates.applications\XmlApp1.xsl
<b>Authentication Settings</b>	
<b>Authorization user name</b>	If access to the target XML file requires authentication, enter the user name needed to access the content.
<b>Authorization password</b>	If access to the target XML file requires authentication, enter the password needed to access the content.
<b>Proxy server</b>	If you are using a proxy to server access the target XML content, enter the address of the proxy.
<b>Proxy server user name/password</b>	If you are using a proxy to access the target XML content, enter the user name and password needed to use the proxy.
<b>Run Tool</b>	Click to initiate the action. The results of the test are displayed in the Results panel.
<b>Save to File</b>	Click to open the Save dialog box and save the results to a file.



# 8

---

## Using Regular Expressions

SiteScope makes use of regular expressions to match text content. Several SiteScope monitors enable for content matching on the text returned from a monitor's request or action. This chapter includes concepts and reference information on using regular expressions to match text content in SiteScope monitors.

### **This chapter includes:**

#### **Concepts**

- Regular Expressions Overview on page 262
- Defining a Regular Expression on page 263
- Matching String Literals on page 264

#### **Reference**

- Matching Patterns with Metacharacters on page 267
- Search Mode Modifiers on page 271
- Retaining Content Match Values on page 273
- SiteScope Date Variables on page 274
- Examples for Log File Monitoring on page 279
- Problems Working with Regular Expressions on page 285

## Regular Expressions Overview

Regular expressions is a name given to a text parsing tool that was developed for use with scripting languages such as Awk and Perl as well as several programming environments such as Emacs, Visual C++, and Java. Regular expressions themselves are not a programming language. They do, however, make use of many special combinations of characters and symbols that often make them more difficult to interpret than some programming languages. The many different combinations of these special characters, known as metacharacters, make regular expressions a very powerful and flexible tool for parsing and isolating specific text within a larger body of text.

Including a regular expression in the **Match content** text box of a monitor instructs SiteScope to parse the text returned to the monitor when it is run and look for content that satisfies the pattern defined by the regular expression. This document presents an overview of the syntax and metacharacters used in regular expressions for use in matching content for SiteScope monitors.

## Defining a Regular Expression

The element of a match content expression in SiteScope is the forward slash (/) character. Entries in the **Match content** text box of a SiteScope monitor must start and end with a forward slash to be recognized as regular expressions. For example, entering the expression `/website/` into the **Match content** box of a monitor instructs SiteScope to search the text content received by the monitor for the literal text string: `website`. If a match is not found, the monitor reports an error status. When a match is found, the monitor reports a good status as long as all other monitor status threshold conditions are also met. If you enter text or other characters into the **Match content** box without delimiting the entry with forward slashes, the entry is either ignored or reported as a content match error by SiteScope.

Adding parentheses ( ) within the forward slashes surrounding the regular expression is another very useful function for regular expressions in SiteScope. The parentheses are used to create a "back reference." As a back reference, SiteScope retains what was matched between the parentheses and displays the text in the **Status** field of the monitor detail page. This is very useful for troubleshooting match content. This is also a way to pass a matched value from one monitor to another or from one step of a URL Sequence Monitor to the next step of the same transaction. Parentheses are also used to limit alternations, as discussed below.

Generally, it is best to use an iterative approach when building regular expressions for content matching with SiteScope. The following are some general steps and guidelines for developing regular expressions for content matches:

- Create a regular expression using literal characters to match a single sample of the data you want to monitor. For example, `/value: 1022.5/`.
- Iteratively replace literal characters with character classes and metacharacters to generalize the literal into a pattern. For example, the literal in the example above could be changed to: `/value:\s\d\d\d\d\d.\d/` to match any four digits, a decimal point, and one more digit.

- ▶ Consider that the pattern of the data you want to match may vary. Adjust your pattern to match expected or possible variations in the target data. Continuing with the example used above, the expression `/value:\s\d\d\d\d.\d/` might become `/value:\s[d]{1, 8}.\[d]{1,2}/`. This pattern allows for variation in the number of digits to the left of the decimal point and the number of digits to the right of the decimal point. It expects that there is a decimal point. See the following sections for more information about the character classes used here.
- ▶ Consider that the literal string or pattern you want to match may appear more than once in the content. Identify unique content that precedes the content you want to match, and add regular expression patterns to make sure that the expression matches that unique content before it tries to match the content you are trying to monitor. In the example used here, the pattern may match the first of several entries that have a similar `/value: numbers/` pattern. By adding a literal to the pattern that matches some static content that delimits the particular data can be used to be sure the match is made for the target data. For example, if the data you want to match is preceded by the text `Open Queries`, this literal can be added to the pattern, along with a pattern for any intervening content: `/Open Queries[\s\W]{1,5} value:\s[d]{1, 8}.\[d]{1,2}/`.

## Matching String Literals

Finding and matching an exact or literal string is the simplest form of pattern matching with regular expressions. In matching literals, regular expressions behave much as they do in search/replace in word processing applications. The example above matched the text `Web site`. The regular expression `/Buy Now/` succeeds if the text returned to the monitor contains the characters `Buy Now`, including the space, in that order.

Note that regular expressions are, by default, case sensitive and literal. This means that the content must match the expression in case and order, including non-alphanumeric characters. For example, a regular expression of `/Website/`, without any modifiers, succeeds only if the content contains the string `Website` exactly but fails even if the content on the page is `website`, `WEBSITE`, or `Web site`. (In the last case the match fails because there is space between the two words but not in the regular expression.)



There are cases where you may want to literally match certain non-alphanumeric characters which are special "reserved" metacharacters used in regular expressions. Some of these metacharacters may conflict with important literals that you are trying to match with your regular expression. For example, the period or dot symbol (`.`), the asterisk (`*`), the dollar sign (`$`), and back slash (`\`) have special meanings within regular expressions. Because one of these characters may be a key part of a particular text pattern you are looking for, you must "escape" these characters in your regular expression so that the regular expression processing treats them as literal characters rather than interpreting them as special metacharacters. To force any character to be interpreted as a literal rather than a metacharacter, add a back slash in front of that character.

For example, if you wanted to find the string `4.99` on a Web page you might create a regular expression of `/4.99/`. While this matches the string `4.99`, it would also match strings like `4599` and `4Q99` because of the special meaning of the period character. To have the regular expression interpret the period as a literal, escape the period with a forward slash as follows: `/4\.99/`. You can add the back slash escape character in front of any character to force the regular expression processing to interpret the character following the back slash as a literal. In general, use this syntax whenever you want to match any punctuation mark or other non-alphanumeric character.

## Using Alternation

Alternation allows you to construct either/or matches where you know that one of two or more strings should appear in the content. The alternation character is the vertical pipe symbol ("|").

The vertical pipe is used to separate the alternate strings in the expression. For example, the regular expression `/(e-mail|e-mail|contact us)/` succeeds if the content contains any one of the three strings separated by the vertical pipes. The parentheses are used here to delimit alternations. In this example, there are no patterns outside of the alternation that must be matched. In contrast, a regular expression might be written as `/(e-mail|e-mail|contact) us/`. In this case, the match succeeds only when any of the three alternates enclosed in the parentheses is followed immediately by a single white space and the word `us`. This is more restrictive than the previous example, but also shows how the parentheses limit the alternation to the three words contained inside them. The match fails even if one or more of the alternates are found but the word `"us"` is not the next word.

## Matching Patterns with Metacharacters

Often you may not know the exact text you need to match, or the text pattern may vary from one session or from one day to another. Regular expressions have a number of special metacharacters used to define patterns and match whole categories of characters. While matching literal alphanumeric characters seems trivial, part of the power of regular expressions is the ability to match non-alphanumeric characters as well. Because of this, it is important to keep in mind that your regular expressions need to account for the presence of non-alphanumeric characters in the content you are searching. This means that characters such as periods, commas, hyphens, quotation marks and even white spaces, must be considered when constructing regular expressions.

This section contains the following topics:

- “Metacharacters Used in Regular Expressions” on page 267
- “Defining Character Classes” on page 268
- “Using Quantifiers” on page 270

### Metacharacters Used in Regular Expressions

Metacharacter	Description
<code>\s</code>	Matches generic white space (that is, the Spacebar key). This metacharacter is particularly useful when combined with a quantifier to match varying numbers of white space positions that may occur between words that you are looking to match.
<code>\S</code>	Matches characters that are NOT white space. Note that the <code>\S</code> is capitalized versus the small <code>\s</code> used to match white space.
<code>.</code>	This is the period or dot character. Generally, it matches all characters. SiteScope considers the dot as a form of character class on its own and therefore it should not be included inside the square brackets of a character class.
<code>\n</code>	Matches the linefeed or newline character.
<code>\r</code>	Matches the carriage return character.

Metacharacter	Description
\w	Matches non-white space word characters, the same as what is matched by character class [A-Za-z0-9_]. It is important to note that the \w metacharacter matches the underscore character but not other punctuation marks such as hyphens, commas, periods, and so forth.
\W	Matches characters other than those matched by \w (lower case). This is particularly useful for matching punctuation marks and non-alphabetic characters such as ~!@#\$%^&*()+={[]];;and including the linefeed character, carriage return, and white space. It does not match the underscore character which is considered a word constituent matched by \w.
\d	Matches digits only. This is equivalent to the [0-9] character class.
\D	Matches non-numeric characters (what \d does not match) plus other characters. Similar to \W but also matches on alphabetic characters. In SiteScope, this generally matches everything, including multiple lines, until it encounters a digit.
\b	Requires that the match have a word boundary (usually a white space) at the position indicated by the \b.
\B	Requires that the match not have a word boundary at the position indicated.

## Defining Character Classes

An important and very useful regular expression construct is the character class. Character classes provide a set of characters that may be found in a particular position within a regular expression. Character classes may be used to define a range of characters to match a single position or, with the addition of a quantifier, may be used to universally match multiple characters and even complete lines of text.

Character classes are formed by enclosing any combination of characters and metacharacters in square brackets: `[ ]`. Character classes create an "any-or-all-of-these" group of characters that may be matched. Unlike literals and metacharacters outside character classes, the physical sequence of characters and metacharacters within a character class has no effect on the search or match sequence. For example, the class `[ABC0123abc]` matches the same content as `[0123abcABC]`.

The hyphen is used to further streamline character classes to indicate a range of letters or numbers. For example, the class `[0-9]` includes all digits from zero to nine inclusive. The class `[a-z]` includes all lower case letters from a to z. You can also create more restrictive classes with the hyphen such as `[e-tE-T]` to match upper or lower case letters from E to T or `[0-5]` to match digits from zero to five only.

The caret character (^) can be used within a character class as a negation or to exclude certain characters from a content match.

### Example Character Classes

Example	Description
<code>[a-zA-Z]</code>	This matches any alphabetic character, both upper case and lower case, from the letter a to the letter z. To match more than one character, append a quantifier after the character class as described below.
<code>[0-9]</code>	This matches any digit from 0 to 9. To match more than one digit, append a quantifier after the character class as described below.
<code>[\w\s]</code>	This matches any alphanumeric character and/or any white space.
<code>[\w^_]</code>	This matches any alphanumeric character, excluding the underscore.

## Using Quantifiers

Another set of metacharacters used in regular expressions provides character counting options. This adds a great deal of power and flexibility in content matching. Quantifiers are appended after the metacharacters and character classes described above to specify against which positions the preceding match character or metacharacter should be matched. For example, in the regular expression `/(contact|about)\s+us/`, the metacharacter `\s` matches on a white space. The plus sign quantifier following the `\s` means that there must be at least one white space between the words `contact` (or `about`) and `us`.

The following table describes the quantifiers available for use in regular expressions. The Quantifier applies to the single character immediately preceding it. When used with character classes, the quantifier is placed outside the closing square bracket of the character class. For example: `[a-z]+` or `[0-9]*`.

Quantifier	Description
?	The question mark means the preceding character or character class may appear once but is optional and not required to appear in the position indicated.
*	The asterisk requires that any number of the preceding character or character class appear in the designated position. This includes zero or more matches.  <b>Note:</b> Care must be used in combining this quantifier with the dot ( <code>.</code> ) metacharacter or a character class including the <code>\W</code> metacharacter, as these are likely to "grab" more content than anticipated and cause the regular expression engine to use up all of the available CPU time on the SiteScope server.

Quantifier	Description
+	The plus sign requires that the preceding character or character class appear at least once.
{min,max}	Using curly braces creates a quantifier range. The range enumerator digits are separated by commas. This construct requires that the preceding character or character class appear at least as many times as specified by the <b>min</b> enumerator up to but no more than the value of the <b>max</b> enumerator. The match succeeds as long as there are at least as many matches as specified by the <b>min</b> enumerator. However, the matching continues up to the number of times specified by the <b>max</b> enumerator or until no more matches are found.

Match content in SiteScope is run against the entire HTTP response, including the HTTP header, which is not normally viewable by using the browser. The HTTP header usually contains several lines of text including words coupled with sequences of numbers. This may cause failure of some otherwise simple content matching on short sets of numbers and letters. To avoid this, identify a unique sequence of characters near the text you are trying to match and include them as literals, where applicable, in the regular expression.

## Search Mode Modifiers

Regular expressions used in SiteScope may include optional modifiers outside of the slashes used to delimit the expression. Modifiers after the ending slash affect the way the matching is performed. For example, regular expression of `/website/i` with the `i` search modifier added makes the match content search insensitive to upper and lower case letters. This would match either `website`, `Website`, `WEBSite`, or even `WEBSITE`.

With the exception of the `i` modifier, some metacharacters and character classes can override search mode modifiers. In particular, the dot (`.`) and the `\W` metacharacters can override the `m` and `s` modifiers, matching content across multiple lines despite the modifier.

More than one modifier can be added by concatenating them together after the closing slash of the regular expression. For example: `/matchpattern/ic` combines both the `i` and `c` modifiers.

## Regular Expression Match Mode Modifiers

Mode Modifier	Description
<code>/i</code>	Ignore case mode. This makes the search insensitive to upper case and lower case letters. This is a useful option especially when searching for matches in the text content of Web pages.
<code>/c</code>	The matched pattern must NOT appear anywhere in content that is being searched. This is a "complement" match, returning an error if the pattern IS found, and succeeding if the pattern is NOT found.
<code>/m</code>	Match across multiple lines WITHOUT ignoring intervening carriage returns and linefeeds. With this modifier you may still need to account for possible linefeeds and carriage returns with a character class such as <code>[\w\W]*</code> or <code>[\s\S\n\r]*</code> . The <code>.*</code> does not match carriage returns or linefeed characters with this modifier.
<code>/s</code>	Consider the content as being on a single line, ignoring intervening carriage returns and linefeed characters. With this modifier, both the <code>[\w\W]*</code> character class and the <code>.*</code> pattern match across linefeeds and carriage returns.



## Retaining Content Match Values

Some monitors, like the URL Monitor and URL Sequence Monitor, have a content match value that is logged and can be used to set error status thresholds. Another purpose of the parentheses `/(match pattern)/` used in regular expression syntax is to determine which text is retained for the Content Match Value. You use this function to use content match values directly as thresholds for determining the error threshold of a URL monitor or URL Sequence monitor.

For example, if the content match expression was

```
/Copyright (\d*)/
```

and the content returned to the monitor by the URL request included the string:

```
... Copyright 2007 by HP
```

then the match is made and the retained content match value would be:

```
2007
```

Under the error-if option at the bottom of the monitor set up page, you could then change the error-if condition from the default of status `!= 200` to content match, then specify the relational operator as `!=`, and then specify the value 1998. This sets the error threshold for this monitor so that whenever the year in the string Copyright is other than 1998, the monitor reports an error. This mechanism could be used to watch for unauthorized content changes on Web pages.

Checking a Web page for links to other URLs can be an important part of constructing URL Sequence Monitors. The following regular expression can be used to match the URL text of a link on a Web page:

```
/a href="?([:\W\s\d\.]*)"?/i
```

This expression matches the href="protocol://path/URLname.htm" for many URLs. The question mark modifiers enable the quotation marks around the HREF= attribute to be optional. The `i` modifier allows the match pattern to be case-insensitive.

Retained or remembered values from content matches can be referenced and used as input for subsequent steps in a URL Sequence Monitor. See the **Match content** section of the URL Sequence Monitor for the syntax used for Retaining and Passing Values Between Sequence Steps.

## SiteScope Date Variables

SiteScope uses specially defined variables to create expressions that match the current date or time. These variables can be used in content match fields to find date-coded content. The General Date Variables are useful for matching portions of various date formats. The Language/Country Specific Date Variables enable you to automatically extend the language used for month names and weekday names to specific countries, based on ISO codes.

This section contains the following topics:

- ▶ “General Date Variables” on page 274
- ▶ “Language/Country Specific Date Variables” on page 276
- ▶ “Special Substitution for Monitor URL or File Path” on page 277

### General Date Variables

The following table lists the general variables:

Variable	Range of Values
\$hour\$	0 - 23
\$minute\$	0 - 59
\$month\$	1 - 12
\$day\$	1 - 31
\$year\$	1000 - 9999
\$shortYear\$	00 - 99
\$weekdayName\$	Sun - Sat
\$fullWeekdayName\$	Sunday - Saturday

Variable	Range of Values
\$0hour\$	00 - 23
\$0minute\$	00 - 59
\$0day\$	01 - 31 (two-digit day format)
\$0month\$	01 - 12 (two-digit month format)
\$monthName\$	Jan - Dec (three-letter month format in English)
\$fullMonthName\$	January - December
\$ticks\$	milliseconds since midnight, January 1, 1970

For example, if the content match search expression was defined as:

```
/Updated on $0month$V$0day$V$shortYear$/
```

and the content returned by the request includes the string:

```
Updated on 06/01/98
```

then the expression would match when the monitor is run on June 1, 1998. The match fails if the content returned does not contain a string matching the current system date or if the date format is different than the format specified.

If you want the time to be before or after the current time, you can add a **\$offsetMinutes=mmmm\$** to the expression, and this offsets the current time by **mmmm** minutes (negative numbers are allowed for going backwards in time) before doing the substitutions.

For example, if the current day is June 1, 2007, and the search expression is:

```
/$offsetMinutes=1440$Updated on $0month$V$0day$V$shortYear$/
```

the content string that would match would be:

```
Updated on 06/02/07
```

Note that the date is one day ahead of the system date.

## Language/Country Specific Date Variables

The following table lists the SiteScope special variables for use with international day and month name matching. The characters LL and CC are placeholders for two-letter ISO 639 language code characters and two-letter ISO 3166 country code characters (see the notes below the table for more details).

Variable	Range of Values
\$weekdayName_LL_CC\$	Abbreviated weekday names for the language (LL) and country (CC) specified (see notes below).
\$fullWeekdayName_LL_C C\$	Full weekday names for the language (LL) and country (CC) specified.
\$monthName_LL_CC\$	Abbreviated month names for the language (LL) and country (CC) specified.
\$fullMonthName_LL_CC\$	Full month names for the language (LL) and country (CC) specified.

CC - an uppercase 2-character ISO-3166 country code. Examples are: DE for Germany, FR for France, CN for China, JP for Japan, BR for Brazil. You can find a full list of these codes at a number of Internet sites, such as: <http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html>.

LL - a lowercase 2-character ISO-639 language code. Examples are: de for German, fr for French, zh for Chinese, ja for Japanese, pt for Portuguese. You can find a full list of these codes at a number of Internet sites, such as: <http://www.ics.uci.edu/pub/ietf/http/related/iso639.txt> or <http://www.dsv.su.se/~jpalme/ietf/language-codes.html>.

For example, if the content match expression was defined as:

```
/$fullWeekdayName_fr_FR$/i
```

and the content returned by the request includes the string:

```
mercredi
```

then this expression would match when the monitor was run on Wednesday.

If you are not concerned with the country-specific language variations, it is possible to use any of the above variables without including the country code. For example:

```
/$fullWeekdayName_fr$/
```

could be used to match the same content as `/$fullWeekdayName_fr_FR$/`.

### **Special Substitution for Monitor URL or File Path**

SiteScope Date Variables are useful for matching content as part of a regular expression. The date variables can also be used as a special substitution to dynamically create URLs or file paths for specific monitors. This is useful for monitoring date-coded files and directories where the URL or file path is updated automatically based on system date information. SiteScope is an example of an application that creates date-coded log files. The log file names include some form of the year, month, and day as part of the file name, such as `File2001_05_01.log`, where the year, month, and date are included.

Based on this example, a new file is created each day. Monitoring the creation, size, or content of the current days file would normally require the file path or URL of the monitor to be manually changed each day. Using the SiteScope date variables and special substitution, SiteScope can automatically update the file path to the current day's log file. By knowing the pattern used in naming the files, you can construct a special substitution string similar to a regular expression that substitutes portions of the system date properties into the file path or URL.

For example if the absolute file path to the current day's log file in a file monitor is:

```
D:/Production/Webapps/Logs/File2001_05_01.log
```

the log file for the following day would be:

```
D:/Production/Webapps/Logs/File2001_05_02.log
```

You can construct a special substitution expression to automatically update the file path used by the monitor, with the following syntax:

```
s/D:\Production\Webapps\Logs\File$year$_$0month$_$0day$.log/
```

The substitution requires that the expression start with a lower-case `s` and that the expression is enclosed by forward slashes `/.../`. Forward slashes that are part of the file path must be escaped by adding the back slash (`\`) character as shown. The SiteScope date variables are separated by the underscore character literals. SiteScope checks the system time properties each time the monitor runs and substitutes with applicable values into the file path or URL before accessing the file.

SiteScope monitor types that support the special substitution are:

- e-Business chain
- File Monitor
- Log Monitor
- URL Monitor
- URL Sequence Monitor
- Web server monitor

While the special substitution syntax is similar in syntax to the substitution syntax used in regular expressions, they are not the same. While all of the SiteScope date variables can be used in match content regular expressions, the special substitution discussed here can not be used as part of a match content expression.

## Examples for Log File Monitoring

SiteScope's Log File Monitor and File Monitor check for entries in files created by other applications. These files may be data files created by a third-party application or they may be logs created by a custom system specially designed for your environment. Where the logs or files are written with a known, predictable format, SiteScope can be configured to regularly check the files for new entries and match on specific content strings. The following are several examples of log file entries and simple regular expression patterns that can be used to check the entries. You can use these examples or modify them to work with a specific case.

---

**Note:** All regular expressions must be entered on a single line in SiteScope. Some of the examples below may break across more than one line to fit on this page.

---

This section contains the following topics:

- “Searching Paths for Log Files” on page 280
- “Matching Comma-Separated Values” on page 281
- “Matching Whitespace Separated Values” on page 282
- “Matching and Retaining the Numbers in a Line of Text and Numbers” on page 283
- “Matching Integers and Floating-point Numbers (Positive or Negative)” on page 283
- “Matching Date and Time Coded Log Entries” on page 284

## Searching Paths for Log Files

UNIX and Windows operating systems treat the case (“N” versus “n”) of file names in incompatible ways. Windows operating systems are case insensitive which means that when a file is being searched, its case is ignored. UNIX operating systems are case sensitive which means that the case of a name is significant at all times. To avoid log file errors when using regular expressions to search for path names on UNIX operating systems, you should use markers to change the character case in the path expression.

Marker	Description
\$L	Allows changing characters between the \$L marker and the \$E marker to lower case.
\$U	Allows changing characters between the \$U marker and the \$E marker to upper case.
\$E	The end marker used for changing character case.

### Example

If you define the following path expression:

```
s/tmp/logs/arcv.log.$weekdayName$/
```

for the `/tmp/logs/arcv.log.tue` log file on a Linux machine, you get a log file error because SiteScope tries to find `tmp/logs/arcv.log.Tue`, and Linux is case sensitive.

To resolve this problem, define the path expression as follows:

```
s/\\tmp\\logs\\arcv.log.$L$weekdayName$$E/
```

The monitor converts the characters between \$L and \$E to lower case, `/tmp/logs/arcv.log.tue`.



Conversely, use \$U and \$E to allow SiteScope to change the characters between the markers to upper case. For example, if you define the path expression:

```
s/\tmp\logs\arcv.log.$L$weekdayName$$E/
```

the monitor converts the path to /tmp/logs/arcv.log.TUE.

You can use \$L and \$U multiple times in a path expression, and you can use them both in the same expression.

For example:

```
s/\tmp\logs-$L$weekdayName$$E\arcv.log.$U$weekdayName$$E/
```

converts the path to /tmp/logs-tue/arcv.log.TUE

```
s/\tmp.$L$monthName$$E\logs-$L$weekdayName$$E\arcv.log.$U$weekdayName$$E/
```

converts the path to /tmp.mar/logs-tue/arcv.log.TUE

## Matching Comma-Separated Values

The following is an example of log file entries that are comma-separated strings of digits and letters:

```
new,open,changed,12>alerts
new,open,changed,13>alerts
new,open,changed,13>alerts
new,open,changed,14>alerts
```

A regular expression to match on log file entries that are comma-separated strings of digits and letters.

```
/([\w\d]+,[\w\d]+,[\w\d]+,[\w\d]+)[\n\r]?/
```

**Note:** If the file entries include punctuation marks such as an underscore or a colon, add that character explicitly to the `[\w\d]` class pattern. For example, to include a colon character, change each of the `[\w\d]` patterns to `[\w\d:]`.

---

## Matching Whitespace Separated Values

The following is an example of log file entries that are a sequence of strings and digits separated by spaces:

```
requests 12 succeeded 12 failed
requests 12 succeeded 12 failed
requests 11 succeeded 11 failed
requests 12 succeeded 12 failed
requests 10 succeeded 10 failed
```

The following is a regular expression to match on log file entries that are a sequence of strings and digits separated by spaces.

```
/([\w\d]+\s+[\w\d]+\s+[\w\d]+\s+[\w\d]+\s+[\w\d]+)[\n\r]?/
```

---

**Note:** The use of the `+` character forces the match to include the number of sequences per line included in the match pattern: in this example, five word or number sequences per line of the log file. If the sequences include punctuation marks such as an underscore or colon, add that character explicitly to the `[\w\d]` class pattern. For example, to include a colon character, change each of the `[\w\d]` patterns to `[\w\d:]`.

---

## Matching and Retaining the Numbers in a Line of Text and Numbers

The following is an example of log file entries that are comma separated strings that combine digits and letters:

```
request handle number 12.56, series 17.5, sequence reported 97.45, 15.95 and 19.51
request handle number 15.96, series 27.5, sequence reported 107.45, 25.95 and 19.52
request handle number 11.06, series 36.5, system codes 9.45, 35.95 and 19.53
log reference number 12.30, series 17.5, channel reset values 100.45, 45.95 and 19.54
```

The following is a regular expression to match on log file entries that are comma-separated strings that combine digits and letters and retain the decimal numeric data:

```
/[,\\w\\s]+(\\d+\\.\\d+)[,\\w\\s]+(\\d+\\.\\d+)[,\\w\\s]+(\\d+\\.\\d+)[,\\w\\s]+(\\d+\\.\\d+)[,\\w\\s]+(\\d+\\.\\d+)[\\n\\r]
?/.
```

---

**Note:** If the file entries include punctuation marks such as an underscore or colon, add that character explicitly to the `[,\\w\\s]` class pattern. For example, to include a colon character that appears embedded in the text sequences, change each of the `[,\\w\\s]` patterns to `[,:\\w\\s]`.

---

## Matching Integers and Floating-point Numbers (Positive or Negative)

The following is an example of log file entries that are a sequence of integers and floating point numbers that may be negative or positive:

```
12.1987 -71 -199.1 145 -1.00716
13.2987 -72 -199.2 245 -1.00726
14.3987 -73 -199.3 345 -1.00736
15.4987 -74 -199.4 445 -1.00746
```

The following is a regular expression to match on log file entries that are a sequence of 5 integers and floating point numbers that may be negative or positive. The numbers in each entry must be separated by one or more spaces.

```
/(-?\d+\.\d{0,})[\s]+(-?\d+\.\d{0,})[\s]+(-?\d+\.\d{0,})[\s]+(-?\d+\.\d{0,})[\s]+(-\d+\.\d{0,})[\n\r]?/
```

## Matching Date and Time Coded Log Entries

Many log files include some form of date and time data with each entry. The following is an example of log file entries that include date and time information together with string data separated by commas:

```
20/04/2003 14:29:22,ERROR,request failed
20/04/2003 14:31:09,INFO,system check complete
20/04/2003 14:35:46,INFO,new record created
```

The following is a regular expression to match on log file entries that are date- and time-coded followed by comma-separated strings of letters and digits. This example uses the SiteScope date variables to match only on entries that were created on the same day, month, and year as indicated by the system clock of the server where SiteScope is running.

```
/${0day}$V${0month}$V${0year}$\s+\d+:\d+:\d+,[\w\d]+,[\w\d]+/
```

The following example uses the SiteScope date variables to match on a more restricted set of entries that were created on the same day, month, year, and within the same hour as indicated by the system clock of the server on which SiteScope is running.

```
/${0day}$V${0month}$V${0year}$\s+${0hour}$:\d+:\d+,[\w\d]+,[\w\d]+/
```

## Problems Working with Regular Expressions

This section contains problems encountered when working with regular expressions.

- **Using the .\* construct presents a very large number of possible matches on any page of content.** The use of the .\* construct is known to cause the regular expression-matching engine used by SiteScope to take over all available CPU cycles on the SiteScope server. If this occurs, SiteScope is unable to function and must be restarted each time the monitor with the offending regular expression is run, until the expression has been corrected.

---

**Note:** Regular expression matching is run against the entire text content returned to the SiteScope monitor request. This includes HTTP headers that are normally not viewable in the browser window (for example, not visible using the **View > Source** option). This also means that you must account for other information that may not be displayed in the browser view. This includes text in META tags used by Internet search engines as well as client side-scripts.

---

- **Text matching is done against the code lines of the script and not against the browser's output from the script for URLs that contain client side-scripts, such as Javascript.** This means that if the script dynamically writes or replaces text on the Web page with values calculated by the script, it may not be possible to match this content with regular expressions. If the script is only changing text, you may be able to match the corresponding text strings that appear in the script code. A further pitfall would be that you are trying to check that a certain condition was met in the browser but the matching text string appears in the script content regardless of any user action.

- ▶ **A regular expression match succeeds as soon as the minimum match requested is satisfied.** After a match is made, no further matching is performed. Therefore, regular expressions are not well suited to count the number of occurrences of a repeating text pattern. For example, if you want to check a Web page with a catalog list of items and each item has a link next to it saying Buy Now! and you want to make sure that at least five items are listed, a regular expression of /Buy Now!/ would succeed in matching only the first Buy Now!. Likewise, if your regular expression searches the word catalog on the main browser screen, the match may succeed if the word appears as a META tag in the HTML header section or if it appears as a hyperlink in a site navigation menu that appears in the content before the occurrence you intend to match.
- ▶ **Forgetting to account for non-alphanumeric content.** Regular expressions need to be written to account for all of the characters that are and may be present. This includes white space, linefeed, and carriage returns. This is not normally a problem when matching a single-word literal. It can be a challenge when you need to create a match of several words separated by unknown amounts of white space and other non-alphanumeric characters and possibly span more than one line. The `[\s\n\r]+` character class can be useful between words used in the expression. Always check the format of the content you are trying to match to look for patterns and special characters, such as periods, commas, and hyphens, that may cause a seemingly simple match to fail.
- ▶ **Use of excessive metacharacters can be problematic.** In some cases, overly generous quantifiers combined with the `.` or `\W` metacharacters can grab content that you were intending to match with a literal string elsewhere in your regular expression resulting in a match failure. For example, the following might be used to match the URL content of the hyperlink anchor reference: `/a href="([\W\w\s]*)"/`. When the monitor performs the check for this regular expression, however, the match grabs the first occurrence of the pattern `/a href="...` and continues matching multiple lines of text up to the last quotation mark found on the page. Without some other unique ending delimiter, the `[\W\w\s]*` class and quantifier combination is too excessive. A more successful syntax that narrows the class of expected characters would be: `/a href="?([:\W\w\s\d\.]*)?/"`

**Example Regular Expression Syntax**

The following are some examples of syntax for use in regular expressions:

Example Expression	Description
/CUSTID\s?=\s?([A-Z0-9]{20,48})/	This example matches an ID string that is made of 20 or more digits and upper-case letters with no spaces or other non-alphanumeric characters. The \s? construct allows a white space on either side of the equals sign. Using the parentheses around the character class instructs SiteScope to retain this value (up to the maximum of 48 characters) as a content match value and the matched value is displayed in the monitor detail status column.
/href="?([:\w\s\d\.]*)"?/i	This example matches the URL string in an HTML hyperlink. The "?" construct makes a quotation mark on either end of the URL string optional. Using the parentheses instructs SiteScope to retain this value as a content match value and the value is displayed in the monitor status. The i modifier tells the search to treat upper- and lower-case letters equally.
/"[^"]*"/	This example matches text sequences that are contained between quotation marks. Note the use of the negation caret (^) to define a character class of all characters other than the quotation mark.

As with programming and scripting languages, there is almost always more than one way to construct a regular expression to accomplish a particular match. There is not one right way to build regular expressions. You should plan to test and modify regular expressions as necessary until you get the results you need.





# Part III

---

## Monitors



# 9

---

## Working with SiteScope Groups

This chapter includes the main concepts, tasks, and reference information for working with SiteScope groups.

### **This chapter includes:**

#### Concepts

- ▶ SiteScope Groups Overview on page 292

#### Tasks

- ▶ Manage a Group – Workflow on page 294

#### Reference

- ▶ SiteScope Groups User Interface on page 296

## SiteScope Groups Overview

You create group containers to make deployment of monitors and associated alerts manageable and effective for your environment and organization. Each SiteScope monitor instance that you create must belong to a SiteScope group, either a top level group or a subgroup nested within other group containers.

For example, if you intend to monitor a large number of processes running on your system, you may want all of them to be in a single group named **Processes**. If you are monitoring processes on several machines using remote monitors, you could create a primary group called **Processes** with several subgroups named after each of the remote machines that you are monitoring.

When you add a new monitor you either add it to an existing group, or you must first create a group for it. You can add groups individually to SiteScope, or you can deploy groups along with multiple monitors by using templates.

This section contains the following topics:

- “Copying or Moving Existing Groups” on page 292
- “Creating Group Alerts and Reports” on page 293

### **Copying or Moving Existing Groups**

In addition to creating groups, you can copy or move existing groups to a new location within the SiteScope tree. Copying or moving a group duplicates the configuration settings for the group and all monitors within the group. After copying or moving a group, you normally need to edit the group and the configuration properties for each individual monitor within the group to direct the monitors to a unique system or application. Otherwise, the monitors in the group duplicate the monitoring actions of the original group.

---

**Notes:**

- ▶ Instead of copying groups which can lead to redundant monitoring, we recommend that you use templates to more efficiently replicate common group and monitor configuration patterns. For more information about working with templates, see “SiteScope Templates”.
  - ▶ To avoid group identity problems within SiteScope, object names must be unique within the parent container. If you copy or move a monitor group to a container in which there is another group with exactly the same name, SiteScope automatically adds a suffix (number) to the end of the monitor group's name.
  - ▶ You cannot move or copy a monitor group to its subgroup.
- 

**Creating Group Alerts and Reports**

After creating a group, you can create alerts and reports for the group. By default, group alerts and reports are associated with all monitors within the group.

You create an alert by adding an alert definition to a group container. This means that when any one monitor in the group reports the status category defined for the alert (for example, error or warning), the group alert is triggered. You can configure a group alert to exclude one or more of the monitors in the group by using the **Alert targets** selection tree. For details on this topic, see “SiteScope Alerts Overview” on page 1960.

You create a group report by adding a report definition to a group container. You can configure a group report to exclude one or more of the monitors in the group by using the **Monitors and groups to report on** selection tree. For details on this topic, see “SiteScope Reports Overview” on page 2035.

If you delete a group, SiteScope removes the applicable monitor actions and disables any alert actions associated with the group.

## **Manage a Group – Workflow**

This task describes the steps involved in managing a group.

This task includes the following steps:


- “Create SiteScope Groups and Subgroups” on page 294
- “Create Monitor Instances” on page 295
- “Add URL Links to Group Description - Optional” on page 295
- “Set Group Dependencies - Optional” on page 295
- “Set Up Group Alerts - Optional” on page 296
- “Set Up Group Reports - Optional” on page 296
- “Results” on page 296

### **1 Create SiteScope Groups and Subgroups**

Create SiteScope groups and subgroups according to the monitor hierarchy which you want to implement in the monitor view. For example, you can create groups of locations, server types, network resources, and so forth.

- **Create a new group.** Right-click the SiteScope or group container in which to create the group, and select **New > Group**. For details on the user interface, see “New SiteScope Group Dialog Box” on page 297.
- **Create a group by copying or moving an existing group.** Right-click the group you want to copy or move, and click **Copy** or **Cut**. Right-click the location in the monitor tree where you want to copy or move the group container, and click **Paste**.

---

**Note:** You can also move or copy multiple monitors and groups to a target group by clicking the **Manage Monitors and Groups** button  in the monitor tree toolbar. For details on the user interface, see “Manage Monitors and Groups Dialog Box” on page 68.

---

## 2 Create Monitor Instances

Select the monitor instances you want to add to the group.

For details on how to perform this task, see “Deploy a Monitor – Workflow” on page 323.

## 3 Add URL Links to Group Description - Optional

You can add additional information to describe a group, and include HTML tags for hyperlinks to enable you to access URLs from the Dashboard.

- a To add a hyperlink, open the Properties tab for the selected group.
- b Expand the **General Settings** panel and enter the URL in the **Group description** field. For example, `<a href="http://www.hp.com">My Link</a>`.
- c Click the **Dashboard** tab. A URL is displayed in the **Description** field for the selected group. To open the URL, click the group’s **Description** field, and then click the link.

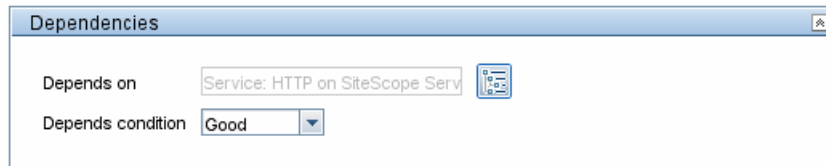
## 4 Set Group Dependencies - Optional

You can set group dependencies to make the running of monitors in this group dependent on the status of another monitor.

For details on this topic, see “Monitoring Group Dependencies” on page 307.

### Example

The monitors in the group being configured run normally as long as the monitor selected in the **Depends on** box reports the condition selected in the **Depends condition** box. In this example, the group being configured is enabled only when the **Service** monitor reports a status of **Good**.



## 5 Set Up Group Alerts - Optional

To create an alert for the group, right-click the group and select **New > Alert**. For each alert scheme, you can create one or more alert actions. In the New Alert dialog box, click **Add Action** to start the Alert Action wizard.

For details on how to perform this task, see “Configure an Alert” on page 1984.

## 6 Set Up Group Reports - Optional

To create a report for the group, right-click the group and click **Reports**. Select a report type and configure the report settings.

For details on how to perform this task, see “Create a Report” on page 2041.

## 7 Results

The monitor group, including its monitors, alerts, and reports, is added to the monitor tree.

## SiteScope Groups User Interface

**This section includes:**

- ▶ New SiteScope Group Dialog Box on page 297



## New SiteScope Group Dialog Box

<b>Description</b>	<p>Enables you to define a new group for SiteScope, or a subgroup for an existing monitor group.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope container or an existing monitor group, and select <b>New &gt; Group</b>.</p>
<b>Important Information</b>	<p>You cannot delete a monitor group if it has dependent alerts or reports at the container level. To delete a monitor group with dependencies, you must remove the monitor group from <b>Alert Targets</b> and <b>Report Targets</b> for each dependency, and then delete the monitor group. You can delete monitor groups that have dependencies at the child level.</p>
<b>Included in Tasks</b>	<p>“Manage a Group – Workflow” on page 294</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Groups Overview” on page 292</li> <li>▶ “Monitor Tree” on page 72</li> </ul>


The following elements are found throughout the New SiteScope Group dialog box:

### General Settings

GUI Element	Description
<b>Group name</b>	<p>Enter a name that describes the content of the group, or the purpose of the monitors added to the group. For example, &lt;host_name&gt; or &lt;business_unitresource_name&gt; or &lt;resource_type&gt;.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ The group name cannot be <b>sitescope</b> or contain any of the following characters: ‘ ; &amp;   &lt; &gt; / \ + =</li> <li>▶ The group name is case sensitive. This means that you can have more than one group with the same name provided they each have a different case structure.</li> </ul>

GUI Element	Description
<b>Group description</b>	<p>Enter additional information to describe a group. This can include the most common HTML tags for text styling, such as &lt;BR&gt;, &lt;HR&gt;, and &lt;B&gt;, and hyperlinks. The description is displayed only when viewing or editing the group's properties in the Dashboard. For details on adding a hyperlink, see "Add URL Links to Group Description - Optional" on page 295.</p> <p><b>Note:</b> This field does not support Javascript/iframes/frames or other advanced features. HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> <li>➤ Tags: <b>script</b>, <b>object</b>, <b>param</b>, <b>frame</b>, <b>iframe</b>.</li> <li>➤ Any tag that contains an attribute starting with <b>on</b> is declined. For example, <code>onhover</code>.</li> <li>➤ Any attribute with <b>javascript</b> as its value.</li> </ul>
<b>Source template</b>	<p>Displays the path of the source template if the group was created from a template. If you are using deployed templates created in older versions of SiteScope, enables you to manually associate the root groups with the source template by entering the path of the source template.</p>
<b>Clear</b>	<p>Click to remove the source template associated with the root group.</p>

## Dependencies

GUI Element	Description
<b>Depends on</b>	<p>Click <b>Depends on</b>  to open the Dependency dialog box, and select the monitor on which you want to make the running of this monitor group dependent.</p> <p>For details on the Dependency dialog box, see “Dependency Dialog Box” on page 377.</p> <p>For details on this topic, see “Monitoring Group Dependencies” on page 307.</p> <p><b>Default:</b> No dependency is set for a monitor group.</p>
<b>Depends condition</b>	<p>Select the <b>Depends condition</b> that the <b>Depends on</b> monitor should have for the current monitor group to run normally. If the selected condition is not satisfied then the monitor selected in the <b>Depends on</b> box is automatically disabled. The conditions are:</p> <ul style="list-style-type: none"> <li>➤ Good</li> <li>➤ Error</li> <li>➤ Available</li> </ul>

## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>
<b>Add Tag</b>	<p>Click to add a new keyword tag.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>

# 10

---

## Working with SiteScope Monitors

This chapter includes the main concepts, tasks, and reference information for working with SiteScope monitors.

### **This chapter includes:**

#### **Concepts**

- ▶ SiteScope Monitors Overview on page 302
- ▶ SiteScope Monitor Categories on page 303
- ▶ Monitoring Remote Servers on page 306
- ▶ Monitoring Group Dependencies on page 307
- ▶ Setting Status Thresholds on page 309
- ▶ Setting Status Thresholds Using a Baseline on page 312

#### **Tasks**

- ▶ Deploy a Monitor – Workflow on page 323
- ▶ Set Monitor Thresholds Using a Baseline on page 327

#### **Reference**

- ▶ Monitor Categories List on page 336
- ▶ Monitors Supported in Windows Environments Only on page 342
- ▶ Monitors Supporting Windows Management Instrumentation (WMI) on page 343
- ▶ Ports Used for SiteScope Monitoring on page 344
- ▶ List of Deprecated SiteScope Monitors on page 349
- ▶ SiteScope Monitors User Interface on page 350

## SiteScope Monitors Overview

SiteScope monitors are tools for automatically connecting to and querying different kinds of systems and applications used in enterprise business systems. The different monitor types provide the generic capabilities for performing actions specific to different systems. You create one or more instances of a monitor type to instruct SiteScope how to monitor specific elements in your IT infrastructure.

For example, you can create 100 monitor instances that instruct the SiteScope CPU Monitor type to connect to and measure CPU utilization on remote servers. Each monitor instance contains a different setting defining which remote server is to be monitored and how often. SiteScope is then configured to automatically monitor the CPU utilization on 100 servers at regular intervals.

Monitor instances that you create must be added within a SiteScope monitor group container. You use group containers to help you organize the monitor instances that you create.

---

**Note:** For a list of counters or metrics that can be configured for SiteScope monitors, as well as versions of applications or operating systems that are supported, see the HP SiteScope Monitors and Metrics document located in `<SiteScope>\sisdocs\pdfs\SiteScope_Monitors_Metrics.doc`.

---

## SiteScope Monitor Categories

SiteScope monitor categories are grouped according to classes that indicates their availability and category that reflect their function. When you select to add a new monitor to a SiteScope agent, the list of available monitor types for that agent are displayed both alphabetically and divided by category in the product interface. The availability of the monitor category is dependent on the class of monitor. This section describes the monitor classes and the category listing formats.

This section contains the following topics:

- “Standard Monitors” on page 303
- “Integration Monitors” on page 304
- “Solution Template Monitors” on page 304

### Standard Monitors

Standard monitor categories represent the monitor categories available with a general SiteScope license. These monitor categories include many of the general purpose monitor categories.

- **Application Monitors.** Monitors in this category monitor 3rd party applications. These monitors enable SiteScope to access and retrieve data from the monitored applications.
- **Database Monitors.** Monitors in this category monitor different types of database applications. There are monitors that access data from specific database applications and generic monitors that can be configured to monitor any database application.
- **Generic Monitors.** Monitors in this category monitor various type of environment. These monitors can monitor networks, applications, and databases depending on how they are configured.
- **Network Monitors.** Monitors in this category monitor network health and availability.
- **Server Monitors.** Monitors in this category monitor server health and availability.

- ▶ **Stream Monitors.** Monitors in this category monitor applications that play media files and stream data.
- ▶ **Web Transaction Monitors.** Monitors in this category monitor web-based applications.
- ▶ **Virtualization Monitors.** Monitors in this category monitor virtualization technologies.

For information about the usage and configuring each monitor type, see the section for the particular monitor category.

To see the list of monitors contained in each monitor category, see “Monitor Categories List” on page 336.

## **Integration Monitors**

This group of optional monitor types are used to integrate HP products with other commonly used Enterprise Management systems and applications.

These monitor types require additional licensing and may only be available as part of another HP product. For more information about Integration Monitor capabilities, see the section on “Working with SiteScope Integration Monitors” on page 1129.

To see the list of monitors contained in each monitor category, see “Monitor Categories List” on page 336.

## **Solution Template Monitors**

Solution template monitor types are a special class of monitors that enable new monitoring capabilities for specific applications and environments. As part of a solution template, these monitor types are deployed automatically together with other, standard monitor types to provide a monitoring solution that incorporates best practice configurations. These monitor types are controlled by option licensing and can only be added by deploying the applicable solution template. After they have been deployed, you can edit or delete them using the same steps as with other monitor types. For more information, see “SiteScope Solution Templates” on page 1665.



The monitor types using solution templates include:

- Active Directory (with and without Global Catalog)
- HP Service Manager
- Microsoft Exchange 5.5, 2000, 2003, 2007
- Microsoft IIS Server
- Microsoft SQL Server
- Microsoft Windows Resources
- Oracle Database 9i and 10g
- SAP Application Server (NetWeaver and R3)
- Siebel Application/Gateway/Web Server (for UNIX and Windows)
- UNIX Resources
- WebLogic Application Server
- WebSphere Application Server

## Monitoring Remote Servers

Some SiteScope monitors use Internet protocols to test Web systems and applications. Other SiteScope monitors use network file system services and commands to monitor information on remote servers.

Monitoring remote Windows servers requires:

- ▶ SiteScope for Windows XP/2000/2003. In general, SiteScope for UNIX cannot monitor remote Windows servers.
- ▶ The SiteScope service must run in a user or administrative account that has permission to access the Windows Performance registry on the remote servers to be monitored. For details on how to change the SiteScope account user, see “Change the User Account of the SiteScope Service” on page 1281.

To monitor certain server level parameters on a remote server using the network files system services, you must create a remote server profile. A table of server profiles is listed on the Microsoft Windows/UNIX Remote Server page in the remote server view. The remote server profiles contain the address and connection information that SiteScope needs to make a remote connection. After creating remote server profiles, set up monitors to use the remote connection profile. For details on creating remote profiles and remotely monitoring either Windows or UNIX servers, see “Remote Servers Overview” on page 1276.

The requirements for monitoring services and applications that are running on remote servers vary according to the application and network policies in your environment. For information about how SiteScope monitors connect to remote systems, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277 and “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285.

You can also check for other information relating to monitoring remote servers in the HP Software Self-solve knowledge base (<http://h20230.www2.hp.com/selfsolve/documents>). To enter the knowledge base, you must log in with your HP Passport ID.

## Monitoring Group Dependencies

To prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system, select one monitor to check the basic availability of the system and then create other monitors that perform more detailed tests of that system. This creates a dependency relationship that enables you to make the running of a monitor group dependent on the status of a selected monitor.

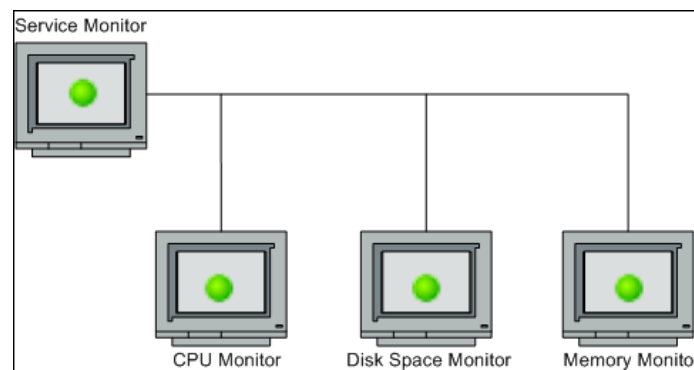
For information about configuring dependency settings, see “Depends on” and “Depends condition” on page 361.

This section contains the following topics:

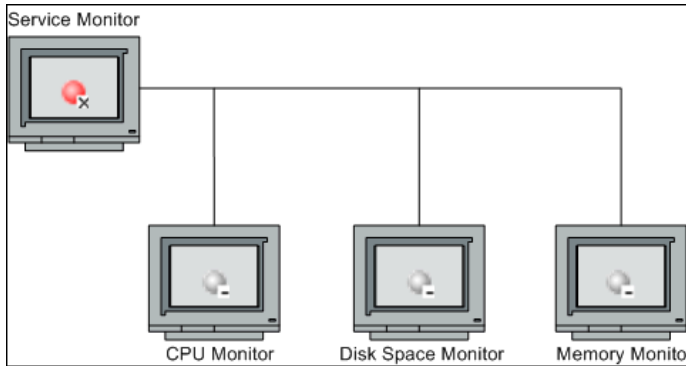
- “Depends On” on page 307
- “Depends Condition” on page 309

### Depends On

You use this option to make the running of this monitor dependent on the status of another monitor. This can be used to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system. You can create a simple system monitor to check the basic availability or heartbeat of a system and then create other monitors that perform more detailed tests of that system. The figure below shows an example dependency relationship where three system monitors have been made dependent on a Service Monitor instance.



The detailed test monitors can be made dependent on the status of the heartbeat monitor by selecting that monitor. This means the dependent monitors run as long as the dependency condition is satisfied. If the heartbeat monitor detects that the target system has become unavailable, the dependency relationship automatically disables the other monitors. This has the effect of disabling any alerts that would have been generated by those monitors. The figure below shows the example monitors are disabled because the monitor on which they depend is reporting an error condition.



By default, no dependency is set for a monitor instance. To make the running of the monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which you want to create dependence, and select the check box next to the required monitor. To remove dependence on a monitor, clear the required check box.

## Depends Condition

If you choose to make a monitor dependent on the status of another monitor (by using the **Depends on** setting), you use this option to select the status category or condition that the **Depends on** monitor should have for the current monitor to run normally.

The status categories include:

- Good
- Error
- Available
- Unavailable

The monitor being configured is run normally as long as the monitor selected in the **Depends on** box reports the condition selected in this box. If you have selected **Unavailable** and the **Depends on** monitor reports this status, the current monitors are not disabled.

For example, by selecting **Good**, this monitor is only enabled as long as the monitor selected in the **Depends on** box reports a status of **Good**. The current monitor is automatically disabled if the monitor selected in the **Depends on** box reports a category or condition other than the condition selected for this setting. See the examples for the **Depends On** setting.

## Setting Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status is based on the results or measurements returned by the monitor action on the target system as compared to the thresholds set for the monitor.

You can set status threshold criteria for each monitor instance to determine an **Error** status, a **Warning** status, and a **Good** status. Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value that you may specify. The parameter and the value depend on the monitor type. For example, the measurement parameter for a CPU monitor is CPU utilization (%).

You can set up one or more status threshold criteria for each status condition. Most monitor types include one default setting for each of the three status conditions. By default, only one threshold is displayed when you first configure the monitor.

This section contains the following topics:

- “Scheduling” on page 310
- “Availability” on page 310
- “Baseline Thresholds” on page 311
- “Threshold Status Impact” on page 311
- “Multiple Thresholds” on page 312
- “Configuring Status Thresholds” on page 312

## Scheduling

You can also select a schedule to determine the status of the monitor instance if you want to define when to check the monitor run result against the threshold. This is useful if you want to restrict checking the monitor run results against the threshold to certain days or hours only. For example, you may want the monitor status to be based on results gathered during business hours only. At times outside the threshold schedule period, the monitor is assigned the predefined status in the **Default status** box. By default, monitor run results are checked against the threshold on an **every day, all day** schedule.

## Availability

When the monitor is not available, it is assigned a status that is based on the user definition in the **If Unavailable** drop-down list. A monitor can have a state of **Unavailable** as well as a status of **Good**, **Warning**, or **Error**. Alerts are triggered according to availability, status, or both availability and status.

## Baseline Thresholds

Instead of setting logic conditions manually in the threshold settings for each monitor instance, you can have SiteScope calculate thresholds for one or more monitor instances using a baseline. For information about this topic, see “Setting Status Thresholds Using a Baseline” on page 312.

## Threshold Status Impact

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the monitor detects that the system has become unavailable, the status change from **Good** to **Error** is used to trigger an alert on error.

A change of status may also affect the state of a dependency between monitors. For example, a monitor that detects a change that results in an **Error** status may be a trigger to disable one or more other monitors that are dependent on the system. For information about dependency settings, see “Monitoring Group Dependencies” on page 307.

The threshold setting also affects the status of the monitor in the SiteScope Dashboard. When viewing SiteScope data in the Current Status tab of Dashboard, you can drill down in the monitor tree to view monitor and measurement status and availability. The status is displayed by color and a status icon in the SiteScope Dashboard. For information on measurement status and availability in the Dashboard user interface, see “Status and Availability Levels” on page 1863.

## Multiple Thresholds

The individual threshold criteria results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status condition setting the status of the monitor is set to the highest valued status condition.

For example, if one condition selected as **Error if** and another condition selected as **Warning if** are both met, the status would be reported as an **Error**, with **Error** being the highest value, **Warning** the next highest and **Good** the lowest value.

## Configuring Status Thresholds

For details on configuring monitor status thresholds, see “Set Monitor Thresholds - Optional” on page 326.

## Setting Status Thresholds Using a Baseline

Baseline data is gathered from monitor performance metrics over a period of time and is used to provide a comparison for establishing acceptable or expected threshold ranges. When the monitor's performance exceeds that range by some value (or does not reach that range, for example, in the case of Free Disk Space), the monitor can signal an error or warning. The acceptable threshold range of a monitor is determined by how far the current performance is from the baseline. Baselines enable you to understand how your applications typically perform and determine whether a performance problem is an isolated incident or a sign of a significant downward performance trend.

For details on this task, see “Set Monitor Thresholds Using a Baseline” on page 327.



This section contains the following topics:

- “Calculating the Baseline” on page 313
- “Activating the Baseline” on page 314
- “Notes and Limitations” on page 315
- “Setting the Baseline Adherence Level” on page 317
- “Understanding the Good and Error Boundaries” on page 317
- “Understanding Baseline Threshold Values” on page 319

## **Calculating the Baseline**

To enable SiteScope to begin calculating baselines, you select the groups and/or monitors to be used for collecting baseline data. You can also select the schedule ranges used for collecting baseline threshold data. This enables you to restrict to certain days or hours of the week the periods during which SiteScope collects data for the baseline calculation. For example, you may want the monitor status to be based on results gathered during peak business hours only.

You can also select the adherence level used for determining the extent to which values for the baseline calculation affect the threshold values and set threshold boundaries for all monitor measurements. For details, see “Setting the Baseline Adherence Level” on page 317 and “Understanding the Good and Error Boundaries” on page 317.

The baseline engine calculates the baseline for each schedule using measurements collected from the monitors during the data collection period. SiteScope uses a percentile algorithm in the baseline calculation, in which a percentile value is used to determine the value of the baseline. For details on how baseline thresholds are calculated, see “Understanding Baseline Threshold Values” on page 319.

## Activating the Baseline

After the baseline is calculated, you can review a summary of calculated monitors and analyze the baseline data in the Activate Baseline dialog box. The dialog box lists all the monitor instances for which a baseline was calculated, the date of the baseline calculation, and the reduction in the number of error and warning statuses that would have been generated for a monitor if the baseline thresholds were applied. If SiteScope is unable to calculate a baseline for a monitor, it lists a reason for calculation failure.

You can also view a graph that displays the current thresholds, the baseline thresholds, and historic data of all baseline-related monitor measurements over a 24-hour time period for each monitor measurement. The graph includes an annotation tool that enables you to annotate a snapshot of the graph you are viewing, to highlight important areas. You can save, print, or email an annotation graph. For details on the user interface, see “Annotation Tool” on page 2085.

After reviewing the baseline data, you can activate baseline threshold configuration. This applies the baseline values to the thresholds for the selected monitors. You can also activate the baseline for monitors that failed for the reason **Insufficient data** by using the limited measurement samples that were collected.

Before activating the baseline threshold, you should consider the option to save the current monitor configuration, because you cannot undo threshold configuration changes after the baseline has been activated.

When the baseline is activated, the baseline thresholds are displayed in the Threshold Settings area for each monitor. Each day when SiteScope restarts, the baseline value is recalculated according to the history samples collected for the measurement and the current day’s readings, and the baseline threshold values are recalculated and updated accordingly.

At any time, you can create a baseline summary report showing the baseline status and baseline status description for each monitor in the selected context.

## Notes and Limitations

- ▶ Only an administrator in SiteScope, or a user granted **Edit monitors** permissions can use the baseline feature to set monitor thresholds, and only for the monitors that are in the users allowed groups list. Any user can view the Baseline Status Report regardless of edit permissions.
- ▶ You cannot add or delete thresholds or measurements, or copy or move monitors during the baseline calculation process (up until the point that the monitor baseline is activated).
- ▶ Before the baseline is calculated, the monitors should be enabled and allowed to run for a period long enough for SiteScope to accumulate sufficient data to calculate the baseline. This period depends on the **Minimum number of days required for baselining** and **Minimum number of samples required for baselining** settings in the Infrastructure Settings Preferences. For details, see “Baseline Settings” on page 1408. The baseline can still be calculated and activated even if the monitor has insufficient data, although the calculation may not be accurate.
- ▶ After you define a set of counters for a browsable monitor and the monitor runs with these counters for some time, if you later change the counters (for example, remove existing counters and/or add new counters), and then you attempt to calculate baseline, the calculation results may be incorrect. This can occur because old data, possibly for counters that no longer exist, interferes with the new data. The calculation may also be incorrect for counters that have not changed since the monitor was created. To avoid this problem, you should not make any changes to a monitor’s browsable counters during the minimum number of days period required for calculating the baseline.
- ▶ You can change threshold related properties using Global Search and Replace, regardless of whether the threshold was created using a baseline or manually. However, you cannot activate a baseline threshold for a monitor using Global Search and Replace.
- ▶ During the baseline calculation and after the baseline is activated, only certain baseline threshold changes are supported. The same restrictions apply when you change threshold related properties using Global Search and Replace. For details on the threshold changes that are allowed, see “Changing Threshold Settings” on page 368.

- ▶ If SiteScope is restarted before the baseline calculation or activation process is complete, it automatically continues the process after the restart. Monitors with any other baseline status (**Calculated, not activated; Activation failed; Calculation failed; Baseline activated**) are not affected by the restart.
- ▶ If SiteScope is restarted before the remove baseline process is complete, the process is not continued after the restart, and you must run the remove baseline process again.
- ▶ If you make changes directly to the SiteScope group .MG files in the **<SiteScope root directory>\groups** directory, only the threshold changes permitted in the user interface are supported (any other changes are ignored). Changes to the baseline status can also be made in the .MG files, but they are not supported.

---

**Note:** SiteScope group .MG files are supported in SiteScope 10.10, however, the **Enable configuration files** option is no longer selected by default when SiteScope is installed. SiteScope group .MG files will be deprecated in SiteScope 11.00.

---

- ▶ Baseline thresholds are not copied or moved along with the other group or monitor objects when copying or moving a group or monitor with an activated baseline.
- ▶ If you click the **Help** button in any of the baseline dialog boxes, you may be prompted to enter your user login credentials.
- ▶ Memory consumption increases for each monitor threshold set using a baseline. To reduce memory consumption, you can set the **Interval for saving accumulated baseline data to disk** settings in the Baseline Settings. For details, see “Baseline Settings” on page 1408.

## **Setting the Baseline Adherence Level**

You can select the baseline adherence level used for determining the threshold value. This is the extent to which values for the baseline calculation affect the threshold values for all monitor measurements. You can select **High adherence**, **Medium adherence**, or **Low adherence**. The higher the adherence level, the closer the threshold range is to the monitor measurement baseline values. Conversely, the lower the adherence level, the further the threshold range is from the monitor measurement baseline values.

In addition to selecting the adherence level, you can also fine-tune the adherence level for individual monitor measurements by configuring adherence percentiles separately for each monitor measurement. Adherence levels are based on adherence percentiles—a measurement value that determines when a measurement is in error or warning. For browsable monitor measurements, you can configure only one set of adherence percentiles that is used by all browsable monitors.

To manually fine-tune the adherence level, you should understand how the threshold values are created. For details on this topic, see “Understanding Baseline Threshold Values” on page 319.

## **Understanding the Good and Error Boundaries**

Configuring good and error boundaries is useful to avoid setting off errors and warnings unnecessarily when using baseline thresholds. You can manually set a good boundary for each monitor measurement and the browsable monitor counters. SiteScope automatically configures the error boundary for each monitor measurement.

---

**Note:** To set good boundaries, it is important to understand how baseline threshold values are created. For details on this topic, see “Understanding Baseline Threshold Values” on page 319.

---

### **Good Boundary**

This is the value of a measurement that is not considered to be in error status, even though according to existing baseline percentiles it should report an error. For example, consider a low load system where CPU utilization measurements are constantly below 3%. Based on these measurements, SiteScope might calculate a baseline threshold with a 5% error threshold. Because this is not an accurate measure of CPU load error, you may want to define 70% CPU utilization as the good boundary to avoid generating false errors. Provided CPU utilization remains below this limit (even though it is above the baseline error threshold), the monitor is not in error status.

You manually set the Good Boundary in the Fine Tune Adherence Levels /Set Boundary dialog box. For details on the user interface, see “Fine-Tune Adherence Levels/Set Boundary Dialog Box” on page 387.

### **Error Boundary**

This is the value of a measurement that is considered to be in error status, even though according to existing baseline percentiles it should not report an error. This can occur when a measurement value grows slowly over a period of time, for example, due to a slow memory leak. Because the baseline threshold is recalculated and updated every day as the measurement average increases, the measurement value does not cross the new threshold.

To overcome this problem, SiteScope automatically sets the error boundary for each monitor measurement. It does this by setting a limit that triggers errors when monitor measurements exceed a specified value, regardless of the baseline. For example, if SiteScope sets an error boundary of 80% CPU utilization, values over 80% CPU utilization are in error status even if the calculated baseline error threshold is not exceeded.

For information on how the error boundary is calculated, see “How SiteScope Calculates the Error Boundary” on page 321.

## Understanding Baseline Threshold Values

To help you fine-tune the percentile value used in the baseline calculation at each adherence level and to set the error and good boundaries (for details, see “Understanding the Good and Error Boundaries” on page 317), it is important to understand:

- the types of threshold values
- how they are applied to measurements
- how measurements are used to calculate baseline thresholds and boundaries

Baseline thresholds are added or updated dynamically to the monitor configuration for each measurement the monitor had before the baseline was calculated. Baseline thresholds are added for each schedule selected for collecting baseline data.

In general, there are two types of thresholds: baseline thresholds and static thresholds. Baseline thresholds have a percentile value that is used to determine when a measurement is in error or warning status, while static thresholds have an actual fixed value. Baseline threshold measurements have a condition of either  $\geq$  or  $\leq$  depending on the direction of the measurement.

Baseline thresholds are changed, added, or deleted on measurements provided the following two conditions are met:

- The measurement can be used in the baseline calculation. To be used in the baseline calculation, a measurement must be numeric and it must have a direction. An example of a measurement that cannot be used in the baseline calculation is a URL 404 error code (it is numeric, but it has no direction).
- The measurement has a static threshold defined for any schedule and any status category (Good, Warning, Error) prior to the baseline calculation.

Measurements that do not adhere to these conditions are not affected (in terms of the thresholds defined on them), and a baseline is not calculated for these measurements.

## How SiteScope Calculates Thresholds

When SiteScope calculates the baseline, it creates a percentile value for each baselinable threshold measurement for each schedule. SiteScope makes an adjustment for extreme measurements by discarding, by default, 2% of the most extreme samples (considered "noise" measurements), and calculates the percentiles on the remaining measurements. For example, if most monitor run results on a server show CPU utilization of no more than 20% and one peak value of 50%, the peak value is not used to determine the baseline. You can change the percentage of discarded measurement samples in the Baseline Settings.

The baseline engine uses a sliding-window approach to calculate thresholds. This means that newer data samples have more influence on the baseline calculation than older samples, and that after a period of time (by default 30 days), the historic data becomes obsolete. You can set the number of days to include in the calculation in the Baseline Settings.

For information about configuring Baseline Settings in the Infrastructure Settings Preferences, see "Baseline Settings" on page 1408.



## How SiteScope Calculates the Error Boundary

SiteScope uses the percentile value to create an error boundary for each measurement. This is the value of a measurement that is considered to be in error status, even though according to existing baseline percentiles it should not report an error. For details, see “Error Boundary” on page 318.

SiteScope calculates the error boundary in one of the following ways:

- ▶ If the measurement has a static error threshold for the specific schedule, the percentile value of the baseline threshold is calculated into an actual value and this value is then compared to the value of the static threshold as follows:

- ▶ If the static error threshold value is more extreme than the baseline threshold value, the static error threshold value is used as the error threshold boundary for that measurement.

**Example:** If the static error threshold is 100% CPU utilization and the computed baseline threshold is 67% CPU utilization, the static error threshold value (100% CPU utilization) is used as the error boundary.

- ▶ If the baseline threshold value is more extreme than the static error threshold value, then the offset value is used. The offset is a percentage value that SiteScope adds to the baseline threshold value (or subtracts from, depending on the direction of the measurement), and the resulting value is used as the error boundary for that measurement. You can determine the offset value in the Baseline Settings area of Infrastructure Settings Preferences.

**Example:** If the static error threshold for a schedule is 60% CPU utilization and the computed baseline threshold value is 65% CPU utilization, the error boundary is calculated as:  
 $65\% \text{ CPU utilization} * 130\%$  (using the default offset value of 0.3) =  
84.5% CPU utilization.

- If there is no error threshold value for the measurement with the specific schedule prior to calculating the baseline (the measurement has a warning or good threshold value but no error threshold value), and the **Automatically create an error boundary if no error thresholds are defined** option is selected in the Baseline Settings, the percentile value of the baseline threshold is calculated into an actual value and the offset value is added to/subtracted from the baseline threshold value (depending on the direction of the measurement). The resulting value is used as the error boundary for the measurement.

---

**Note:** An error boundary is not created if:

- There is no error threshold value for the measurement with the specific schedule prior to calculating the baseline (for example, the measurement has a warning or good threshold value but no error threshold value), and
- The **Automatically create an error boundary if no error thresholds are defined** option is not selected.

---

For details on defining the offset value and automating error boundary creation, see “Baseline Settings” on page 1408.

## Deploy a Monitor – Workflow

This task describes the steps involved in deploying a monitor.

- “Prerequisites” on page 323
- “Create Monitor Instances” on page 324
- “Add URL Links to Monitor Description - Optional” on page 324
- “Set Monitor Dependencies - Optional” on page 325
- “Set Monitor Thresholds - Optional” on page 326
- “Set Up Monitor Alerts - Optional” on page 327
- “Set Up Monitor Reports - Optional” on page 327
- “Results” on page 327

### 1 Prerequisites


- Monitors can be created in a SiteScope group only. For details on how to create a group, see “Create SiteScope Groups and Subgroups” on page 294.
- To enable SiteScope to monitor data on remote servers, you must configure remote servers.
  - For details on enabling SiteScope to monitor data on remote Windows servers, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
  - For details on enabling SiteScope to monitor data on remote UNIX servers, see “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285.
- Check if there are setup requirements and user permissions that need to be obtained for the monitor before configuring the monitor. For details, see the help for the specific monitor.

## 2 Create Monitor Instances

You can create new monitor instances, or copy or move existing monitor instances to the group in the monitor view.

- ▶ **Create a new monitor.** Right-click the group into which you want to add the monitor instance, and select **New > Monitor**. Select the monitor you want to add from the New Monitor Page, and complete the monitor properties form. For details on the user interface, see “New Monitor Page” on page 351.
- ▶ **Create a monitor by copying or moving an existing monitor.** Right-click the monitor you want to copy or move, and click **Copy** or **Cut**. Right-click the location in the monitor tree where you want to copy or move the monitor, and click **Paste**. After copying a monitor, you normally need to change the system or application that the monitor is targeting, otherwise the copied monitor duplicates the monitoring actions of the original monitor instance.

---

**Note:** You can also move or copy multiple monitors and groups to a target group by clicking the **Manage Monitors and Groups** button  in the monitor tree toolbar. For details on the user interface, see “Manage Monitors and Groups Dialog Box” on page 68.

---

## 3 Add URL Links to Monitor Description - Optional

You can add additional information to describe a monitor, and include HTML tags for hyperlinks to enable you to access URLs from the Dashboard.

- To add a hyperlink, open the **Properties** tab for the selected monitor.
- Expand the **General Settings** panel and enter the URL in the **Monitor description** field. For example, `<a href="http://www.hp.com">My Link</a>`.
- Click the **Dashboard** tab. A URL is displayed in the **Description** field for the selected monitor. To open the URL, click the monitor's **Description** field, and then click the link.

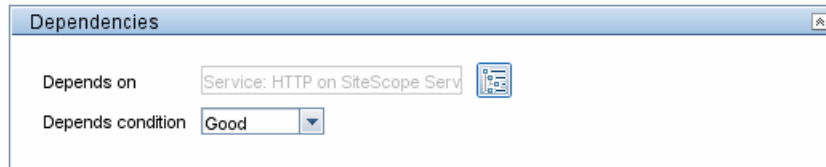
## 4 Set Monitor Dependencies - Optional

You can set monitor dependencies to make the running of this monitor dependent on the status of another monitor.

For details on how to set monitor dependencies, see “Dependencies” on page 360.

### Example

The monitor being configured is run normally as long as the monitor selected in the **Depends on** box reports the condition selected in the **Depends condition** box. In this example, the monitor being configured is enabled only when the **Service** monitor reports a status of **Good**.



The screenshot shows a window titled "Dependencies" with a close button in the top right corner. Inside the window, there are two rows of configuration options:

- The first row is labeled "Depends on" and contains a text input field with the value "Service: HTTP on SiteScope Serv" and a small icon to its right.
- The second row is labeled "Depends condition" and contains a dropdown menu with "Good" selected and a downward-pointing arrow.

## 5 Set Monitor Thresholds - Optional

You can manually set logic conditions that determine the reported status of each monitor instance, or you can set thresholds for one or multiple monitors using a baseline.

- ▶ For details on the user interface for setting monitor thresholds manually, see “Threshold Settings” on page 362.
- ▶ For details on how to set monitor thresholds using a baseline, see “Set Monitor Thresholds Using a Baseline” on page 327.

### Example

If you are monitoring a CPU and acceptable thresholds are 60%-90%, set the threshold settings as follows:

Error if	<input type="checkbox"/>	utilization(%)	>=	90	every day, all day	<input type="checkbox"/>	New Error if
Warning if	<input type="checkbox"/>	utilization(%)	>=	60	every day, all day	<input type="checkbox"/>	New Warning if
Good if	<input type="checkbox"/>	always (default)	<	60	every day, all day	<input type="checkbox"/>	New Good if

CPU utilization of less than 60% results in a good status; CPU utilization equal to or greater than 60% but lower than 90% results in a warning status; CPU utilization equal to or greater than 90% results in an error status.

## 6 Set Up Monitor Alerts - Optional

To create an alert for the monitor, right-click the monitor and select **New > Alert**. For each alert scheme, you can create one or more alert actions. In the New Alert dialog box, click **Add Action** to start the Alert Action wizard.

For details on how to perform this task, see “Configure an Alert” on page 1984.

## 7 Set Up Monitor Reports - Optional

To create a report for the monitor, right-click the monitor and click **Reports**. Select a report type and configure the report settings.

For details on how to perform this task, see “Create a Report” on page 2041.

## 8 Results

The monitor is added to the specified monitor group in the monitor tree.

## Set Monitor Thresholds Using a Baseline

This task describes the steps involved in setting monitor thresholds using a baseline.

This task includes the following steps:

- “Prerequisites” on page 328
- “Configure Baseline Settings Preferences - Optional” on page 328
- “Calculate the Baseline” on page 328
- “Review the Baseline Settings” on page 331
- “View the Baseline Monitor Measurements Graphs” on page 332
- “Activate the Baseline Settings” on page 333
- “View Baseline Properties in the Baseline Status Report” on page 334
- “View and Modify Baseline Thresholds” on page 335

## 1 Prerequisites

Before calculating a baseline for a monitor, make sure that the monitor is enabled and has run for a period long enough for SiteScope to accumulate sufficient data to calculate the baseline. This period depends on the minimum number of days and samples required to calculate the baseline which you configure in the Baseline Settings. For details on the user interface, see “Baseline Settings” on page 1408.

---

**Note:** The baseline can still be calculated and activated even if the monitor has insufficient data, although the calculation may not be accurate.

---

## 2 Configure Baseline Settings Preferences - Optional

You can view and define the values of global SiteScope baseline settings in Infrastructure Settings Preferences. This includes calculation and activation priority settings, the number of days of historical data to include in baseline calculations, and the offset for calculating the error boundary.

For details on the user interface, see “Baseline Settings” on page 1408.

## 3 Calculate the Baseline

Define thresholds on the monitor measurements for which the baseline should be calculated.

- a** Select the monitor instances you want to baseline. For details on the user interface, see “Select Monitors for Baseline Calculation” on page 384.
- b** Select one or more schedule ranges to be used for collecting baseline data, or accept the default schedule (**every day, all day**). For details on the user interface, see “Schedule” on page 385.
- c** Select the global baseline adherence level that is used for determining the extent to which values for the baseline calculation affect the threshold values for all monitor measurements. For details on the user interface, see “Adherence Level” on page 385.



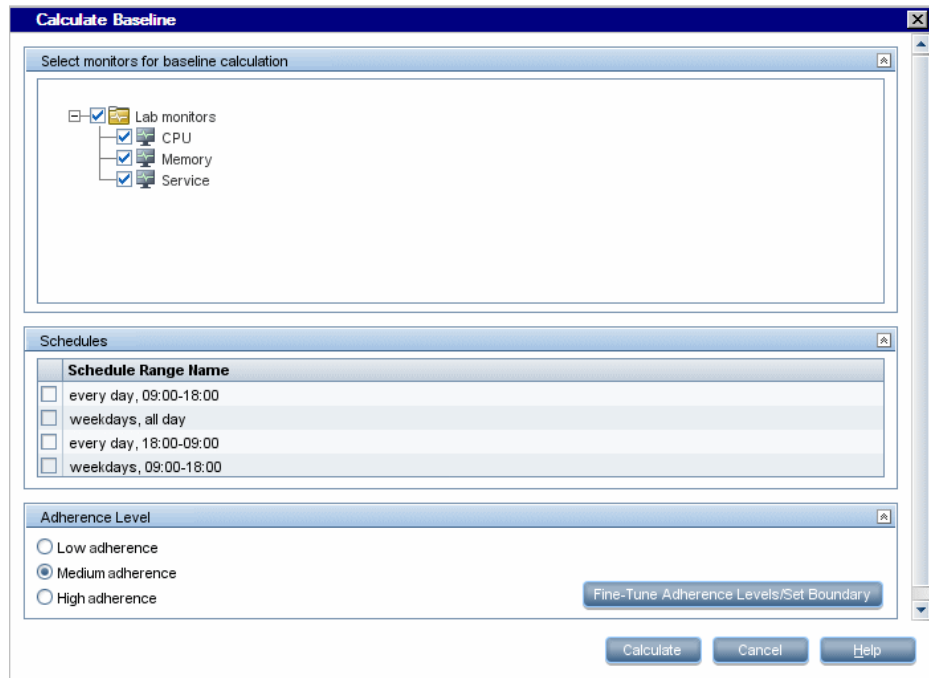
**d** Additionally, you can click the **Fine-Tune Adherence Levels/Set Boundary** button to:

- Individually fine-tune the baseline adherence level for any monitor measurement.
- Define a good boundary for each monitor measurement. A measurement within this boundary is not in error status, even though it should report an error according to existing baseline percentiles.

For details on the user interface, see “Configure Adherence Percentiles” on page 387.

**e** Click **Calculate** to perform the baseline threshold calculation.

### Example - Calculate Baseline Dialog Box





**Note:** Only those monitors that the user is eligible to see according to their user permissions are displayed.

**Example - Fine-Tune Adherence Levels/Set Boundary Dialog Box**



**Fine-Tune Adherence Levels/Set Boundary**

Monitors With Static Counters

Reset  

Monitor Name : Measurement Name	Warning Percentiles			Error Percentiles			Good Boundary
	Low	Medium	High	Low	Medium	High	
CPU : utilizationPercentage	110	93	90	120	98	95	
CPU : utilizationPercentage1	110	93	90	120	98	95	
CPU : utilizationPercentage2	110	93	90	120	98	95	
Web Server : lastHitsPerMinute	110	93	90	120	98	95	
Web Server : lastBytesPerMinute	110	93	90	120	98	95	

Browsable Monitors

Reset  

Monitor Name : Measurement Name	Warning Percentiles			Error Percentiles			Good Boundary
	Low	Medium	High	Low	Medium	High	
All browsable monitor's measurements	110	93	90	120	98	95	

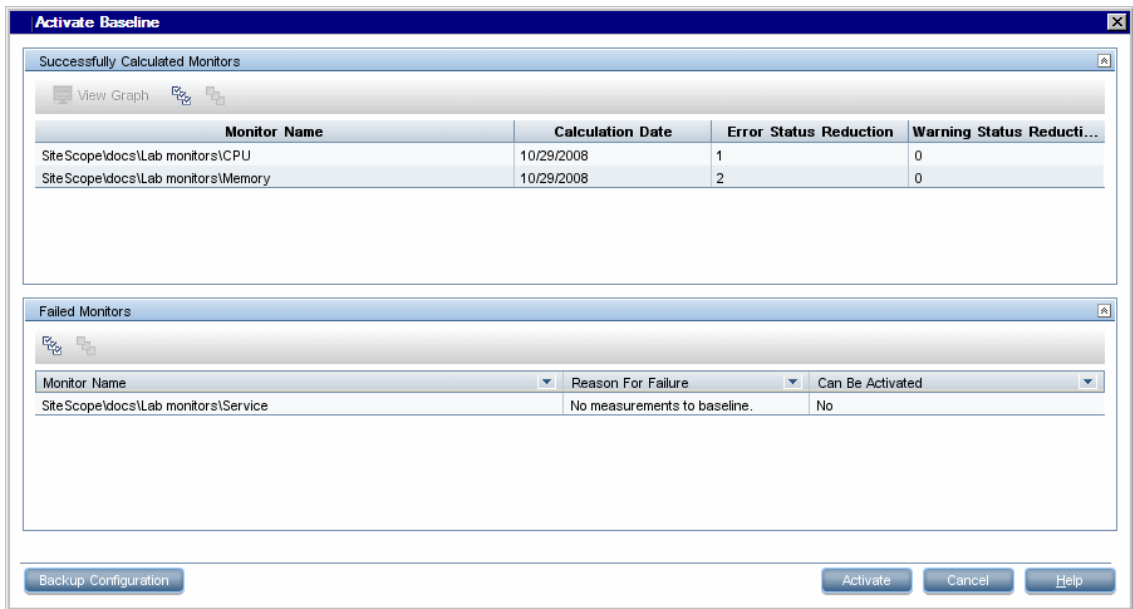
Save Cancel Help

## 4 Review the Baseline Settings

Review the summary of calculated monitors and baseline data in the Activate Baseline dialog box. Only the monitors that the user is eligible to see according to their user permissions are displayed.

For details on the user interface, see “Activate Baseline Dialog Box” on page 389.

### Example




---

**Note:** Only those monitors that the user is eligible to see according to their user permissions are displayed.

---

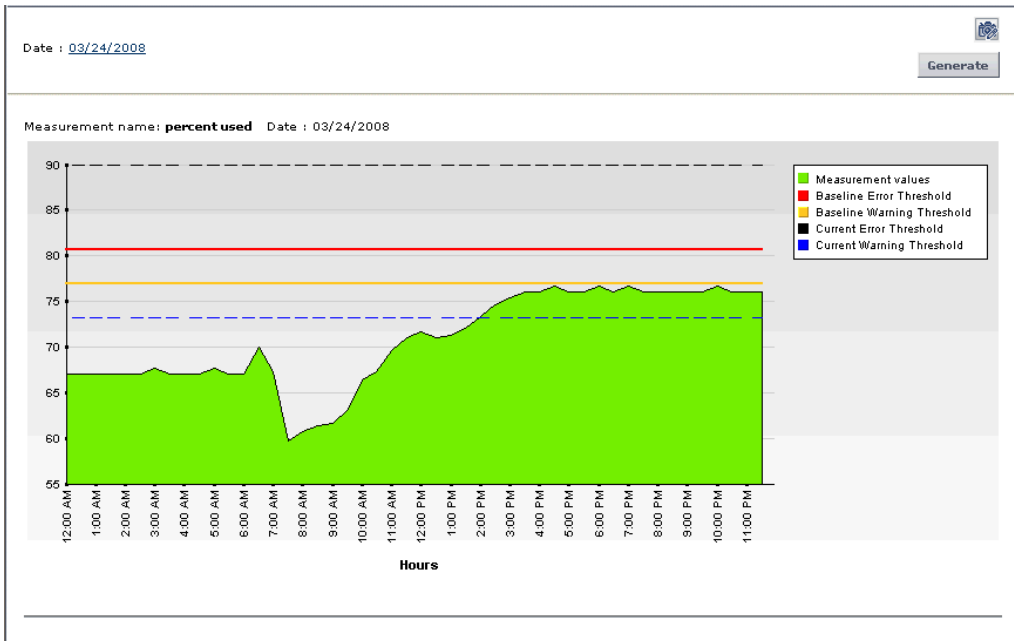
## 5 View the Baseline Monitor Measurements Graphs

You can view a graphical display of each monitor’s baselined measurements to analyze the baseline data for a selected day. You can also use the annotation tool to create a snapshot of the graph you are viewing and highlight important areas.

For details on the user interface, see “Baseline Monitor Measurement Graphs Dialog Box” on page 394.

**Note:** The data displayed in the graphs is an aggregate of the measurement data and as such, the time periods may not accurately reflect the time the data was actually collected.

### Example



## 6 Activate the Baseline Settings

Select the monitors for which you want to set thresholds using a baseline, and click **Activate**. You can select all monitors with a successfully calculated baseline, and those that failed with the reason **Insufficient data** (indicated by **Yes** in the **Can Be Activated** column). The monitor thresholds are configured according to the baseline calculation, and are set to change status when the thresholds settings are exceeded.

For details on the user interface, see “Activate Baseline Dialog Box” on page 389.

---

**Note:** If you want to revert to the current monitor threshold configuration, select the option to save the current monitor configuration before activating the baseline configuration.

---

## 7 View Baseline Properties in the Baseline Status Report

You can create an ad hoc report showing information about each monitor in the selected context, including each monitor's baseline status and baseline status description. For details on the user interface, see “Baseline Status Report” on page 399.

You can also track the baseline status for a monitor in the monitor's Baseline Settings. For details on the user interface, see “Baseline Settings” on page 376.

### Example - Baseline Status Report


Baseline Status Report			
Summary			
<b>Total of 10 monitors.</b> <b>2 monitors have an activated baseline.</b> <b>The calculation failed for 1 monitor.</b> <b>7 monitors are not baselined.</b>			
Details			
Monitor Name	Monitor Type	Baseline Status	Baseline Status Details
SiteScope\AutoSanity\Basic\Disabl...	CPU	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\CPU U...	CPU	Baseline activated	
SiteScope\AutoSanity\Basic\Memo...	Memory	Calculation failed	No measurements to baseline
SiteScope\AutoSanity\Basic\FTP o...	Port	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\URL L...	URL List	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\Disk S...	Disk Space	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\Direct...	Directory	Baseline activated	
SiteScope\AutoSanity\Basic\Link C...	Link Check	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\ Servi...	Service	Monitor not selected for baselining	
SiteScope\AutoSanity\ddd:ddd	CPU	Monitor not selected for baselining	

## 8 View and Modify Baseline Thresholds

In the Threshold Settings, you can view the baseline thresholds and manually fine-tune the thresholds by changing the percentile value from which the threshold value is derived.

For details on the user interface, see “Threshold Settings” on page 362.

### Example



In the example, the Error if percent used threshold value is  $\geq 42.81$  and the Warning if percent used threshold value is  $\geq 40.77$  (both these values are non-editable). To change the threshold values, you must change the percentile value from which the threshold values are derived. To help you understand what the new threshold value is after you change the percentile value, click the **Percentiles Table**  button to open the percentile table that shows the threshold value that is mapped to each percentile range.


Threshold Settings
✖

If unavailable Set monitor status according to Thresholds ▾



Default status Good ▾


Error if



Condition	Operator	Value	Schedule
percent used ▾	$\geq$ ▾	42.81 	every day, all day ▾
percent used ▾	$=$ ▾	'n/a'	every day, all day ▾
percent used (default) ▾	$>$ ▾	90	every day, all day ▾

Warning if

Condition	Operator	Value	Schedule
percent used ▾	$\geq$ ▾	40.77 	every day, all day ▾

Good if

Condition	Operator	Value	Schedule
always (default) ▾	$\geq$ ▾		every day, all day ▾

**Note:** The **Error if percent used (default) > 90** threshold is the error boundary. This is the value of a measurement considered to be in error status, even though according to existing baseline percentiles it should not report an error. For example, if the baseline threshold were updated to **Error if percent used (%) >= 96**, all measurements greater than 90 are in error status, even if the calculated baseline error threshold of 96 is not exceeded. For details on this topic, see “Error Boundary” on page 318.

---

## Monitor Categories List

This section includes the following tables that display the SiteScope monitors in each monitor category:

- “Application Monitors” on page 337
- “Database Monitors” on page 338
- “Generic Monitors” on page 339
- “Network Monitors” on page 339
- “Server Monitors” on page 340
- “Stream Monitors” on page 340
- “Web Transaction Monitors” on page 341
- “Virtualization Monitors” on page 341
- “Integration Monitors” on page 341



## **Application Monitors**

- Active Directory Replication Monitor
- Apache Server Monitor
- BroadVision Application Server Monitor
- Check Point Monitor
- Cisco Works Monitor
- Citrix Monitor
- ColdFusion Server Monitor
- COM+ Server
- F5 Big-IP Monitor
- Microsoft ASP Server Monitor
- Microsoft Exchange 2003 Mailbox Monitor
- Microsoft Exchange 2003 Public Folder Monitor
- Microsoft Exchange 2000/2003/2007 Message Traffic Monitor
- Microsoft Exchange 2007 Monitor
- Microsoft Exchange 5.5 Message Traffic Monitor
- Microsoft IIS Server Monitor
- News Monitor
- Oracle 9i Application Server Monitor
- Oracle 10g Application Server Monitor
- Radius Monitor
- SAP CCMS Monitor
- SAP CCMS Alerts Monitor
- SAP Java Web Application Server Monitor
- SAP Performance Monitor
- SAP Work Processes Monitor

- Siebel Application Server Monitor
- Siebel Log File Monitor
- Siebel Web Server Monitor
- SunONE Web Server Monitor
- Tuxedo Monitor
- UDDI Monitor
- WebLogic Application Server Monitor
- WebSphere Application Server Monitor
- WebSphere MQ Status Monitor
- WebSphere Performance Servlet Monitor

### **Database Monitors**

- DB2 8.x and 9.x Monitor
- Database Counter Monitor
- Database Query Monitor'
- LDAP Monitor
- Microsoft SQL Server Monitor
- Oracle Database Monitor
- Sybase Monitor

## **Generic Monitors**

- Composite Monitor
- Directory Monitor
- File Monitor
- JMX Monitor
- Log File Monitor
- Multi Log File Monitor
- Script Monitor
- Web Service Monitor
- XML Metrics Monitor

## **Network Monitors**

- DHCP Monitor
- DNS Monitor
- FTP Monitor
- Formula Composite Monitor
- Mail Monitor
- MAPI Monitor
- Microsoft Windows Dial-up Monitor
- Network Bandwidth Monitor
- Ping Monitor
- Port Monitor
- SNMP Monitor
- SNMP Trap Monitor
- SNMP by MIB Monitor

### **Server Monitors**

- Browsable Windows Performance Monitor
- CPU Monitor
- Disk Space Monitor
- HP NonStop Event Log Monitor
- HP NonStop Resources Monitor
- IPMI Monitor
- Memory Monitor
- Microsoft Windows Event Log Monitor
- Microsoft Windows Performance Counter Monitor
- Microsoft Windows Resources Monitor
- Microsoft Windows Services State Monitor
- Service Monitor
- UNIX Resources Monitor
- Web Server Monitor

### **Stream Monitors**

- Microsoft Windows Media Player Monitor
- Microsoft Windows Media Server Monitor
- Real Media Player Monitor
- Real Media Server Monitor

## **Web Transaction Monitors**

- e-Business Transaction Monitor
- Link Check Transaction Monitor
- URL Monitor
- URL Content Monitor
- URL List Monitor
- URL Sequence Monitor
- Web Script Monitor

## **Virtualization Monitors**

- Solaris Zones Monitor
- VMware Performance Monitor

## **Integration Monitors**

- HP OM Event Monitor
- HP Service Manager Monitor
- NetScout Event Monitor
- Technology Database Integration Monitor
- Technology Log File Integration Monitor
- Technology SNMP Trap Integration Monitor
- Technology Web Service Integration Monitor

## **Monitors Supported in Windows Environments Only**

The following lists the monitors that are supported in SiteScopes that are running on Windows versions only. Where relevant, the monitors can monitor remote servers running on any platform/operating system.

- ▶ Browsable Windows Performance Monitor
- ▶ Citrix Monitor
- ▶ ColdFusion Server Monitor
- ▶ MAPI Monitor
- ▶ Microsoft ASP Server Monitor
- ▶ Microsoft Exchange 2003 Mailbox Monitor
- ▶ Microsoft Exchange 2003 Public Folder Monitor
- ▶ Microsoft Exchange 2000/2003/2007 Message Traffic Monitor
- ▶ Microsoft Exchange 2007 Monitor
- ▶ Microsoft Exchange 5.5 Message Traffic Monitor
- ▶ Microsoft IIS Server Monitor
- ▶ Microsoft SQL Server Monitor
- ▶ Microsoft Windows Dial-up Monitor
- ▶ Microsoft Windows Event Log Monitor
- ▶ Microsoft Windows Media Player Monitor
- ▶ Microsoft Windows Media Server Monitor
- ▶ Microsoft Windows Performance Counter Monitor
- ▶ Microsoft Windows Resources Monitor
- ▶ Microsoft Windows Services State Monitor
- ▶ Network Bandwidth Monitor
- ▶ Real Media Player Monitor
- ▶ Real Media Server Monitor
- ▶ SiteScope Server Health Monitor

- Sybase Monitor
- Tuxedo Monitor
- Web Script Monitor

## **Monitors Supporting Windows Management Instrumentation (WMI)**

The following lists the monitors that support the Windows Management Instrumentation (WMI) method for collecting data. WMI is a more secure communication method than NetBIOS for gathering management data from remote servers running on Windows servers.

- ColdFusion Server Monitor
- CPU Monitor
- Disk Space Monitor
- Memory Monitor
- Microsoft ASP Server Monitor
- Microsoft IIS Server Monitor
- Microsoft SQL Server Monitor
- Microsoft Windows Media Server Monitor
- Microsoft Windows Resources Monitor
- Microsoft Windows Services State Monitor
- Real Media Server Monitor
- Service Monitor

For details on how to configure the WMI service on the remote machine, see “Configure the WMI Service for Remote Monitoring” on page 1284.

## Ports Used for SiteScope Monitoring

The following table lists the network ports that are generally used for SiteScope monitoring. In many cases, alternate ports may be configured depending on the security requirements of your environment.

Monitor Type	Ports Used
Apache Server Monitor	Port which Apache Server Admin pages located. Configurable by using server configuration file.
BroadVision Application Server Monitor	Uses the Object Request Broker (ORB) port number for the BroadVision server you are trying to monitor.
Check Point Monitor	SNMP monitor. Default is port 161. This is configurable.
Cisco Works Monitor	Cisco Works resources are usually available by using port 161 or 162 (SNMP), depending on the configuration of the server.
Citrix Monitor	Ports 137, 138, and 139 (NetBIOS).
ColdFusion Server Monitor	Ports 137, 138, and 139 (NetBIOS).
CPU Monitor	For local CPU, no ports required. For CPUs on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS). For CPUs on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).
Database Query Monitor	This is configurable and depends on ODBC or JDBC driver and DB configuration.
DB2 8.x and 9.x Monitor	Default is port 50000. This is configurable.
DHCP Monitor	Default is port 68.



Monitor Type	Ports Used
Directory Monitor	<p>For local directory, no ports required.</p> <p>For directories on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS).</p> <p>For directories on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).</p>
Disk Space Monitor	<p>For local disk space, no ports required.</p> <p>For disk space on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS).</p> <p>For disk space on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).</p>
DNS Monitor	Default is port 53.
F5 Big-IP Monitor	Uses SNMP. This is configurable.
File Monitor	<p>Local disk. No ports required.</p> <p>For files on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS).</p> <p>For files on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).</p>
FTP Monitor	Default is port 21. This is configurable.
LDAP Monitor	The default is port 389. This is configurable.
Link Check Transaction Monitor	The default is port 80. This is configurable.
Log File Monitor	<p>Ports 137, 138, and 139 (NetBIOS) for Windows based systems.</p> <p>Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.</p>
Mail Monitor	Port 110 for POP3, port 25 for SMTP, port 143 for IMAP.

Monitor Type	Ports Used
MAPI Monitor	MAPI uses the Name Service Provider Interface (NSPI) on a dynamically assigned port higher than 1024 to perform client-directory lookup.
Memory Monitor	Ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Microsoft ASP Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft IIS Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft SQL Server Monitor	Ports 137, 138, and 139 (NetBIOS).
Microsoft Windows Event Log Monitor	Ports 137, 138, and 139 (NetBIOS).
Microsoft Windows Media Player Monitor	Same port as media content to be monitored.
Microsoft Windows Media Server Monitor	Ports 137, 138, and 139 (NetBIOS).
Microsoft Windows Performance Counter Monitor	Ports 137, 138, and 139 (NetBIOS).
Network Bandwidth Monitor	No ports required; monitors only the local machine.
News Monitor	Default is port 144. This is configurable.
Oracle Database Monitor	This is configurable. Depends on target DB. Default is port 1521.
Oracle 9i Application Server Monitor/Oracle 10g Application Server Monitor	This is configurable. Port which Webcaching admin page located.
Ping Monitor	Default is port 7.

Monitor Type	Ports Used
Port Monitor	Monitors any port.
Radius Monitor	Currently supports Password Authentication Procedure (PAP) authentication but not the Challenge Handshake Authentication Protocol (CHAP) or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). The RADIUS servers must be configured to accept PAP requests. Default is port 1645. In recent changes to the RADIUS spec, this may be changed to 1812. The monitor is configurable.
Real Media Player Monitor	Uses Real Media client on SiteScope box. Uses the port from which the media content is streamed (based on the URL).
Real Media Server Monitor	Ports 137, 138, and 139 (NetBIOS).
SAP CCMS Monitor	Uses SAP Client software (SAP Front End) to run certain SAP transactions. Therefore, same ports as SAP.
Script Monitor	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Service Monitor	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
SNMP Monitor	Default is port 161. This is configurable.
SNMP Trap Monitor	Uses port 162 for receiving traps. This is configurable.
SunONE Web Server Monitor	URL to the stats-xml file on the target SunONE server. The port is configurable.

Monitor Type	Ports Used
Sybase Monitor	Monitor requires Sybase Central client on the machine where SiteScope is running to connect to the Adaptive Server Enterprise Monitor Server. Port number the same as Sybase client.
Tuxedo Monitor	The default port for the TUXEDO workstation listener is port 65535. This is configurable.
URL Monitor	Generally port number 80. This is configurable.
Web Server Monitor	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Web Service Monitor	This is configurable.
WebLogic Application Server Monitor	BEA WebLogic Application Server monitor uses the Java JMX interface. Port is configurable.
WebSphere Application Server Monitor	Same port as the IBM WebSphere Administrator's Console.
WebSphere Performance Servlet Monitor	WebSphere Performance Servlet. Port is configurable.

## List of Deprecated SiteScope Monitors

In recent versions of SiteScope, a number of monitors were deprecated and are no longer supported. The following table lists the deprecated monitors, and where available, the respective monitors that can replace them.

Deprecated Monitor	Recommended Alternative Monitor
Active Directory Performance	N/A
Asset	N/A
Astra Load Test	Web Script
DB2	DB2 8.x and 9.x
Dynamo	N/A
IPlanet Application Server	SunONE Web Server
IPlanet Server	SunONE Web Server
IPlanet Web Server	SunONE Web Server
Network	Network Bandwidth
Quick Test Pro	Web Script
RTSP	Real Media Player
SAP	SAP Performance
SAP Portal	SAP CCMS
SilverStream Server	N/A
WebLogic 5.x Application Server	N/A

For SiteScope upgrade purposes, you can check if the current configuration has any deprecated monitors using the End of Life Monitor Viewer. For details on using the End of Life Monitor Viewer, see “Using the End of Life Monitor Viewer” in the *HP SiteScope Deployment Guide* PDF.

For a list of deprecated Technology Integration monitors, see “List of Deprecated Integration Monitors” on page 1142.

## **SiteScope Monitors User Interface**

**This section includes:**

- ▶ New Monitor Page on page 351
- ▶ Common Monitor Settings on page 354
- ▶ Dependency Dialog Box on page 377
- ▶ Select Template Dialog Box on page 378
- ▶ Copy to Template Tree Dialog Box on page 379
- ▶ Percentile Range Mapping Table on page 381
- ▶ Calculate Baseline Dialog Box on page 383
- ▶ Fine-Tune Adherence Levels/Set Boundary Dialog Box on page 387
- ▶ Activate Baseline Dialog Box on page 389
- ▶ Backup Configuration Dialog Box on page 393
- ▶ Baseline Monitor Measurement Graphs Dialog Box on page 394
- ▶ Remove Baseline Dialog Box on page 398
- ▶ Baseline Status Report on page 399

 **New Monitor Page**

<b>Description</b>	Enables you to define a new monitor in a monitor group. <b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group and select <b>New &gt; Monitor</b> .
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors can be created only in a SiteScope group.</li> <li>▶ You cannot delete a monitor if it has dependent alerts or reports at the container level. To delete a monitor with dependencies, you must remove the monitor from <b>Alert Targets</b> and <b>Report Targets</b> for each dependency, and then delete the monitor. You can delete monitors that have dependencies at the child level.</li> <li>▶ The Monitor description field supports HTML tags (HTML version 3.2) including the most common tags for text styling, such as &lt;BR&gt;, &lt;HR&gt;, and &lt;B&gt;, and hyperlinks. It does not support Javascript/iframes/frames or other advanced features.</li> </ul>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	“Monitor Tree” on page 72

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Quick Search</b>	<p>Enter a monitor name in the <b>Quick Search</b> box. You can select the following settings to help you with your search:</p> <ul style="list-style-type: none"> <li>➤ <b>All.</b> Search for matches in all columns.</li> <li>➤ <b>Monitor.</b> Search for matches in the Monitor column only.</li> <li>➤ <b>Category.</b> Search for matches in the Category column only.</li> <li>➤ <b>Case sensitive.</b> Search for matches that are case sensitive.</li> <li>➤ <b>Case insensitive.</b> Search for matches that are not case sensitive.</li> <li>➤ <b>Use wild cards.</b> Enables you to use wild card characters in your search. For example, use an asterisk wildcard (*) to represent a string of characters, or a question mark wild card (?) to represent one character only.</li> <li>➤ <b>Match from start.</b> Search for monitors/monitor categories that match the search text from the start.</li> <li>➤ <b>Match exactly.</b> Search for monitors/monitor categories that exactly match the search text.</li> <li>➤ <b>Match anywhere.</b> Search for monitors/monitor categories that contain the search text somewhere in the name.</li> </ul>
<b>Recently Used Monitors</b>	<p>Select a monitor from a display of monitors that were recently added to SiteScope monitor groups.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ The five most recently selected monitors are listed here.</li> <li>➤ The displayed monitors may change as more selections are made.</li> </ul>



GUI Element	Description
<b>Available Monitors</b>	<p>Select a monitor to deploy by selecting it from the list of available monitors or by category. To select by category, click the arrow to the right of the <b>Category</b> heading, and select a monitor category from the list detailed below.</p> <p>You can change the alphabetical order (ascending or descending) of the listed monitors or categories, by clicking the arrow in the header of the <b>Monitor</b> or <b>Category</b> column.</p>
<b>Category</b>	<p>You can add a monitor by selecting one of the following categories, and clicking a monitor in that category:</p> <ul style="list-style-type: none"> <li>➤ All (default)</li> <li>➤ Application</li> <li>➤ Database</li> <li>➤ Generic</li> <li>➤ Integration</li> <li>➤ Network</li> <li>➤ Server</li> <li>➤ Stream</li> <li>➤ Web Transaction</li> <li>➤ Virtualization</li> </ul>

## Common Monitor Settings

<b>Description</b>	Enables you to configure settings for a new monitor. <b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b> , and select a monitor from the New Monitor page.
<b>Important Information</b>	HTML code entered in the monitor description fields is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected.
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	“Monitor Tree” on page 72

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Setting panels>	<p>The following setting panels in the monitor Properties tab are common to all monitors. For details on the settings for a specific SiteScope monitor, see the user interface page for the monitor type.</p> <ul style="list-style-type: none"> <li>➤ “General Settings” on page 356</li> <li>➤ “Monitor Run Settings” on page 358</li> <li>➤ “Dependencies” on page 360</li> <li>➤ “Threshold Settings” on page 362</li> <li>➤ “Link Monitor to CI” on page 369</li> <li>➤ “HP BAC Integration Settings” on page 370</li> <li>➤ “Enable/Disable Monitor” on page 373</li> <li>➤ “Enable/Disable Associated Alerts” on page 374</li> <li>➤ “Search/Filter Tags” on page 375</li> <li>➤ “Baseline Settings” on page 376</li> </ul>

GUI Element	Description
<b>Verify &amp; Save</b>	<p>Verifies the correctness of the monitor configuration locally and on the remote server to be monitored, before saving the settings. If SiteScope fails to connect to the remote server, or if there is an invalid property in the configuration settings, verification fails and an error message is displayed.</p> <p><b>Note:</b> Performance is slower if you verify and save than if you just saving the configuration settings, because SiteScope must establish a connection and verify the settings on a remote server. Due to these performance issues, bulk operations such as Publish Template Changes and Global Search and Replace use the save option only.</p>
<b>Save</b>	<p>Performs a local verification of the configuration settings, and saves the settings (without verifying the correctness of the monitor configuration on the remote server).</p> <p><b>Note:</b> Performance is faster than if you verify and save configuration settings, because SiteScope does not need to establish a connection and verify the settings on a remote server.</p>

## General Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Name</b>	<p>Enter a name that describes the element or system being monitored. Use a useful naming convention for all monitors to make creating view filters and category assignments more effective.</p> <p><b>Example:</b> &lt;hostname:resource_type&gt; or &lt;business_unit resource_name monitored_element&gt;</p> <p><b>Default value:</b> SiteScope creates a default name based on the host, system, and/or URL being monitored or the default name defined for the monitor type.</p>

GUI Element	Description
<b>Monitor description</b>	<p>Enter additional information to describe a monitor. This can include the most common HTML tags for text styling, such as &lt;BR&gt;, &lt;HR&gt;, and &lt;B&gt;, and hyperlinks. The description is displayed only when viewing or editing the monitor's properties in the Dashboard. For details on adding a hyperlink, see "Add URL Links to Monitor Description - Optional" on page 324.</p> <p><b>Note:</b> This field does not support Javascript/iframes/frames or other advanced features. HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> <li>➤ Tags: <b>script, object, param, frame, iframe.</b></li> <li>➤ Any tag that contains an attribute starting with <b>on</b> is declined. For example, onhover.</li> <li>➤ Any attribute with <b>javascript</b> as its value.</li> </ul>
<b>Report Description</b>	<p>Enter an optional description for this monitor to make it easier to understand what the monitor does. This description is displayed on each bar chart and graph in Management Reports.</p> <p><b>Example:</b> Network traffic or main server response time.</p> <p><b>Note:</b> HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> <li>➤ Tags: <b>script, object, param, frame, iframe.</b></li> <li>➤ Any tag that contains an attribute starting with <b>on</b> is declined. For example, onhover.</li> <li>➤ Any attribute with <b>javascript</b> as its value.</li> </ul>

 **Monitor Run Settings**


The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Frequency</b>	<p>Set how often SiteScope attempts to run the action defined for the monitor instance. Each monitor run updates the status of the monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p><b>Default value:</b> 10 minutes</p> <p><b>Minimum value:</b> 15 seconds</p> <p><b>Note:</b> When configuring this setting in a template, the variable value can only be in time units of seconds.</p>
<b>Error frequency</b>	<p>Set a new monitoring interval for monitors that have reported an error condition.</p> <p><b>Example:</b> You may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected. When the monitor's status is no longer in error, the monitor reverts to the run interval specified in the <b>Frequency</b> setting.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ Increasing the monitor run frequency affects the number of alerts generated by the monitor.</li> <li>▶ When configuring this setting in a template, the variable value can only be in time units of seconds.</li> </ul>
<b>Verify error</b>	<p>Select to automatically run the monitor again if it detects an error.</p> <p><b>Note:</b> We recommend using this option in small monitoring environments only. Significant monitoring delays may result if multiple monitors are rescheduled to verify errors at the same time.</p> <p>The status returned by the Verify error run of the monitor replaces the status of the originally scheduled run that detected an error. The data from the verify run may be different than the initial error status, causing the loss of important performance data.</p>

GUI Element	Description
<b>Monitor schedule</b>	<p>Select a range schedule if you want the monitor to run only on certain days or on a fixed schedule. The range schedules created in <b>Schedule Preferences</b> appear in the drop-down list. For more information about creating monitor schedules, see “Schedule Preferences Overview” on page 1487.</p> <p><b>Default value:</b> every day, all day</p> <p><b>Note:</b> If you select a threshold schedule in the Threshold Settings, at least one threshold schedule must coincide with the monitor run schedule (at least one minute of the monitor run schedule must be covered by one of the threshold schedules).</p>
<b>Show run results on update</b>	<p>Whenever a change is made to a monitor’s configuration settings, the monitor is run. Select this option to display the results of that monitor run in a popup dialog box.</p> <p><b>Note:</b> The updated run results are always displayed in the applicable dashboard views for the monitor.</p>

## Dependencies

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Depends on</b>	<p>Click <b>Depends on</b>  to open the Dependency dialog box, and select the monitor on which you want to make the running of this monitor dependent. For details on the Dependency dialog box, see “Dependency Dialog Box” on page 377.</p> <p>Use this option to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system.</p> <p><b>Example:</b> Create a system monitor to check the basic availability of a system and then create other monitors that perform more detailed tests of that system. Set the detailed test monitors to be dependent on the status of the monitor checking basic availability.</p> <p>If the system monitor detects that the target system has become unavailable, the dependency relationship automatically disables the other monitors. This also disables any alerts that would have been generated by the dependent monitors.</p> <p><b>Default value:</b> No dependency is set for a monitor instance.</p>





GUI Element	Description
<b>Depends condition</b>	<p>If you make this monitor dependent on the status of another monitor (by using the <b>Depends on</b> setting), use this option to select the status condition of the <b>Depends on</b> monitor for the current monitor to run normally.</p> <p>The status categories include:</p> <ul style="list-style-type: none"> <li>➤ <b>Good</b></li> <li>➤ <b>Error</b></li> <li>➤ <b>Available</b></li> <li>➤ <b>Unavailable</b></li> </ul> <p>The monitor being configured is run normally as long as the monitor selected in the <b>Depends on</b> box reports the condition selected in this box.</p> <p><b>Example:</b> Select <b>Good</b> and this monitor is enabled only when the monitor selected in the <b>Depends on</b> box reports a status of <b>Good</b>. The current monitor is automatically disabled if the monitor selected in the <b>Depends on</b> box reports a category or condition other than <b>Good</b>. You can also enable dependent monitors specifically for when a monitor detects an error.</p> <p><b>Default value:</b> Good</p>

 **Threshold Settings**

<b>Description</b>	<p>Use to set conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system during a specified period of time.</p> <p>Status threshold criteria for each monitor instance can be set for the following status conditions:</p> <ul style="list-style-type: none"> <li>➤ <b>Error if</b></li> <li>➤ <b>Warning if</b></li> <li>➤ <b>Good if</b></li> </ul> <p><b>Note:</b> You can also set monitor thresholds using a baseline. For details, see “Setting Status Thresholds Using a Baseline” on page 312.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>➤ You can apply multiple status threshold criteria for each status condition per monitor instance. A single monitor instance may have one or more criteria used to determine <b>Error</b> status, one or more conditions to determine <b>Warning</b> status, and one or more conditions to indicate <b>Good</b> status. Most monitor types include one default setting for each of the three status conditions.</li> <li>➤ When setting a baseline threshold, you can only change certain threshold conditions during the baseline calculation and after the baseline is activated. For details on the threshold changes that are allowed, see “Changing Threshold Settings” on page 368.</li> <li>➤ When working with Global Search and Replace, if you select to replace threshold settings, the <b>Override Category</b> option appears. When selected, all the threshold settings for the selected monitor instances are overridden with the settings you entered for the replace operation. If this option is cleared and you selected to replace threshold settings, the settings you entered are added to the existing threshold settings for the monitor instances.</li> </ul>


<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>➤ “Deploy a Monitor – Workflow” on page 323</li> <li>➤ “Set Monitor Thresholds Using a Baseline” on page 327</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Setting Status Thresholds” on page 309</li> <li>➤ “Setting Status Thresholds Using a Baseline” on page 312</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Click this button to configure additional thresholds that determine the <b>Error/Warning/Good</b> status. For each threshold, select the measurement and operator, and enter a value for the measurement.</p> <p>By default, two thresholds are displayed for the <b>Error</b> status when you first configure the monitor, and one threshold for the <b>Warning</b> and <b>Good</b> status.</p>
	Click this button to delete the selected threshold.

GUI Element	Description
<p><b>If unavailable</b></p>	<p>Select a status assignment for when the monitor is not available from the following options:</p> <ul style="list-style-type: none"> <li>▶ <b>Set monitor status according to thresholds.</b> The monitor gets a new status according to the thresholds.</li> <li>▶ <b>Set monitor status to Good.</b> The monitor’s status is set to Good when it is unavailable without thresholds being checked.</li> <li>▶ <b>Set monitor status to Warning.</b> The monitor’s status is set to Warning when it is unavailable without thresholds being checked.</li> <li>▶ <b>Set monitor status to Error.</b> The monitor’s status is set to Error when it is unavailable without thresholds being checked.</li> </ul> <p><b>Note:</b> A monitor instance can have a status of <b>Unavailable</b> as well as a status of <b>Good, Warning, or Error</b>. Alerts are triggered according to availability, status, or both availability and status, depending on how the alert is configured. For details, see “SiteScope Alerts Overview” on page 1960.</p>
<p><b>Default status</b></p>	<p>The status of the monitor (<b>Good, Warning, or Error</b>) if the threshold criteria for the monitor instance are not met.</p> <p><b>Default value:</b> Good</p>

GUI Element	Description
<b>On internal error</b>	<p>Select a status assignment for the monitor if a configuration or internal error occurs:</p> <ul style="list-style-type: none"> <li>▶ <b>Set monitor status according to Thresholds.</b> The monitor's status is set according to its current thresholds if a configuration or internal error occurs (default setting). It is unreliable to rely on the threshold since there is no way of knowing at what point the error occurred (and whether the threshold is based on old data, updated data, or both). For example, a monitor may remain in its current status even though the monitor did not actually run; change status if thresholds were defined that were not applicable; or trigger false alerts as if a remote was not available, when in fact, the remote was not contacted.</li> <li>▶ <b>Set monitor status to Error.</b> The monitor's status is set to Error if a configuration or internal error occurs without thresholds being checked.</li> <li>▶ <b>Set monitor status to Warning.</b> The monitor's status is set to Warning if a configuration or internal error occurs without thresholds being checked.</li> <li>▶ <b>Set monitor status to Good.</b> The monitor's status is set to Good if a configuration or internal error occurs without thresholds being checked.</li> <li>▶ <b>Set monitor status to Unavailable.</b> The monitor's status is set to Unavailable if a configuration or internal error occurs without thresholds being checked.</li> </ul>
<b>Error if</b>	Set the conditions for the monitor instance to report an <b>Error</b> status.
<b>Condition</b>	<p>Select the measurement parameter from the drop-down list to determine the status of this monitor instance. The list of measurements is dynamically updated based on the type of monitor you are configuring.</p> <p><b>Default value:</b> Default measurements exist for many monitor types and differ per monitor type. For many default measurements, there are corresponding defaults for the operator and value boxes that are not editable.</p>

GUI Element	Description
<p><b>Operator</b></p>	<p>Select an operator for the measurement from the drop-down list. The following operators are available:</p> <ul style="list-style-type: none"> <li>➤ &gt;= Greater than or equal to</li> <li>➤ &gt; Greater than</li> <li>➤ == Equals</li> <li>➤ != Not the same as</li> <li>➤ &lt;= Less than or equal to</li> <li>➤ &lt; Less than</li> <li>➤ <b>contains</b> Contains the value entered</li> <li>➤ <b>!contains</b> Does not contain the value entered</li> </ul>
<p><b>Value</b></p>	<p>Enter a value applicable to the measurement parameter.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ If a monitor has an activated baseline, its measurement values are non-editable and the <b>Percentiles Table</b>  button is displayed. You can change baseline threshold values by clicking the button and changing the current percentile value from the Percentiles Table. For details on the user interface, see “Percentile Range Mapping Table” on page 381.</li> <li>➤ You cannot change the measurement value, operator or schedule for a baseline threshold condition.</li> </ul>

GUI Element	Description
<b>Schedule</b>	<p>Select a range schedule to determine the status of this monitor instance if you want to define when to check the monitor run result against the threshold. This is useful, for example, if you want to check the monitor run result against the threshold only on certain days or during peak hours. The range schedules created in <b>Schedule Preferences</b> appear in the drop-down list. For more information about creating monitor schedules, see “Schedule Preferences Overview” on page 1487.</p> <p><b>Default value:</b> every day, all day</p> <p><b>Note:</b> When selecting threshold schedules, at least one threshold schedule must coincide with the <b>Monitor schedule</b> in the Monitor Run Settings (at least one minute of the monitor run schedule must be covered by one of the threshold schedules).</p>
<b>Warning if</b>	<p>Set the conditions for the monitor instance to report a <b>Warning</b> status. For each threshold, select the measurement and operator, and enter a value for the measurement.</p>
<b>Good if</b>	<p>Set the conditions for the monitor instance to report a <b>Good</b> status. For each threshold, select the measurement and operator, and enter a value for the measurement.</p>

## Changing Threshold Settings

You can make changes to threshold conditions according to the baseline status of the monitor instance.

Monitor Baseline Status	Change Threshold Condition	Add/Delete Threshold Condition
<b>Not baselined</b>	You can change any condition of any threshold.	Allowed
<b>In calculating/ activating process</b>	You can only change the measurement value for static thresholds. For example, Error if CPU $\geq$ 70 every day, all day, you can only change the value 70 to another value.	Not allowed
<b>Baselined</b>	<ul style="list-style-type: none"> <li>➤ You can change any condition for static thresholds.</li> <li>➤ You can change the percentile value only for baseline thresholds.</li> </ul>	Allowed for static thresholds only



## Link Monitor to CI

**Note:** The Link Monitor to CI settings panel is displayed only when SiteScope is accessed from HP Business Availability Center's System Availability Management Administration page. Technology monitors do not have this setting because the monitors' topologies are reported through their topology settings scripts.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Select CIs button</b>	<p>You can link between this monitor instance and any existing, logical configuration item (CI) in HP Business Availability Center's Universal configuration management database. This link or relationship enables the monitor to pass KPI status to the CI to which it is linked. This is in addition to the monitor's corresponding CI that is created automatically when the monitor instance is created.</p> <p>The Select CIs button opens the dialog box in which you select an existing CI from a CMDB view to link to this monitor instance. For details on selecting and working with views, see "Working with the CI Selector" in <i>Reference Information</i> in the HP Business Availability Center Documentation Library.</p> <p><b>Note:</b> The Link Monitor to CI Settings are available only when editing a SiteScope monitor from System Availability Management Administration and cannot be set while adding a monitor or when working in SiteScope standalone.</p>

## HP BAC Integration Settings

**Note:** The HP BAC Integration Settings panel is displayed only when SiteScope is reporting to HP Business Availability Center.

<b>Description</b>	Use the HP BAC Integration Settings area to control what data a monitor forwards to the HP Business Availability Center database.
<b>Important Information</b>	Your selection should be based on how much data is relevant to report to Business Availability Center for this monitor and how much space the Business Availability Center database has for this data.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>BAC Logging Options</b>	
<b>Disable reporting to BAC</b>	Select when you do not want any of the status information or measurements for this monitor to be transferred to HP Business Availability Center or to temporarily disable reporting this monitor to Business Availability Center.
<b>Enable reporting monitor status and measurements</b>	Select to send all monitor data to HP Business Availability Center for each time that the monitor runs. This option enables the largest data transfer load. <b>Default value:</b> Selected
<b>Enable reporting monitor status (no measurements)</b>	Select this option to send only monitor category ( <b>error</b> , <b>warning</b> , <b>good</b> ), status string, and other basic data for each time that the monitor runs. No information on specific performance counters is included.

GUI Element	Description
<b>Enable reporting monitor status and measurements with thresholds</b>	Select to send monitor category ( <b>error, warning, good</b> ), status string, as well as performance counter data for only those measurement counters that have configured thresholds (for example, Error If, Warning If, Good if). The data is sent for each time that the monitor is run.
<b>Enable reporting changes in status</b>	Select to send only monitor category ( <b>error, warning, good</b> ), status string, and other basic data only when the monitor reports a change in status. No information on specific performance counters is included. This option enables the smallest data transfer load.

GUI Element	Description
<b>Topology Settings</b>	
<p><b>Include topology data when reporting to BAC</b></p>	<p>Selecting this option enables SiteScope to report topology data to Business Availability Center's CMDB. The data that SiteScope forwards depends on the monitor type. This option enables SiteScope to:</p> <ul style="list-style-type: none"> <li>▶ Discover topologies and forward specific CI data for the monitors that monitor applications from among a group of supported environments. For details and a list of these supported environments, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160.</li> <li>▶ Report host CI data for those monitors that monitor hosts. If this option is selected, the monitor creates a topology that includes the host as a CI in Business Availability Center's CMDB.</li> </ul> <p>If cleared, the monitor creates the standard topology of monitor CI (SiteScope monitor) and measurement CI (for only SAP and Siebel environments).</p> <p>For details on how SiteScope reports data to the CMDB, see “Integrating SiteScope Data with HP Business Availability Center's Configuration Items” on page 155.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ This setting does not appear when creating or editing Technology Integration monitors. Those monitors report topologies based on their topology settings scripts.</li> <li>▶ This setting does not appear for those monitors that do not monitor hosts. For a list of these monitors, see “Monitors Without Host Data” on page 168.</li> </ul>

 **Enable/Disable Monitor**

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Enable monitor</b>	If the monitor has previously been disabled, select to enable the monitor. <b>Default value:</b> Selected
<b>Disable monitor</b>	When a monitor has been disabled, SiteScope continues to schedule the monitor to run based on the <b>Frequency</b> setting for the monitor but the monitor action is not run. SiteScope records a monitor data log entry for the monitor when it was scheduled to be run but reports the monitor status as disabled in the place of measurement data.
<b>Disable monitor for the next &lt;time period&gt;</b>	Enter a time period that the monitor should remain disabled. Select <b>Seconds, Minutes, Hours, or Days</b> to define the disable time period as applicable.
<b>Disable monitor on a one time schedule from &lt;time&gt; to &lt;time&gt;</b>	Use this option to temporarily disable the monitor for a time period in the future. The time period can span more than one day. Enter or select the start time and end time for the disable period using the format: hh:mm:ss mm/dd/yyyy.
<b>Disable description</b>	Enter optional descriptive text. This description appears as part of the monitor status in the monitor group display. The disable status text also includes a string indicating which disable option is in force for the monitor, for example Disabled manually indicates that the monitor was disabled using the <b>Disable monitor</b> option.

 **Enable/Disable Associated Alerts**

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Enable all associated alerts</b>	If the alerts associated with this monitor have previously been disabled, select to enable the alerts. <b>Default value:</b> Selected
<b>Disable all associated alerts for the next &lt;time period&gt;</b>	Enter a time period that the associated alerts should remain disabled. Select <b>Seconds, Minutes, Hours, or Days</b> to define the disable time period as applicable.
<b>Disable all associated alerts on a one time schedule from &lt;time&gt; to &lt;time&gt;</b>	Use this option to temporarily disable the associated alerts for a time period in the future. The time period can span more than one day. Enter the start time and end time for the disable period using the format: hh:mm:ss mm/dd/yyyy.
<b>Disable description</b>	Enter optional descriptive text.

 **Search/Filter Tags**

<b>Description</b>	Enables you to add a new search/filter tag, and assign the tag to objects in the context tree and preference profiles.  Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.
<b>Important Information</b>	You can edit existing tags in the Preferences context ( <b>Preferences &gt; Search/Filter Tags</b> ). For details on this topic, see “Search/Filter Tags Overview” on page 1533.
<b>Included in Tasks</b>	“Create and Define a New Search/Filter Tag” on page 108
<b>Useful Links</b>	“Working with Search/Filter Tags” on page 107

The following elements are included (unlabeled GUI elements are shown in

<b>GUI Element</b>	<b>Description</b>
<b>&lt;Tag name and values&gt;</b>	Displays the tag names and tag values if tags have been created. Select the tags or tag values that you want to assign to the object. If no tags have been created for the SiteScope, this section appears but is empty.
<b>Add Tag</b>	Click to add a new keyword tag.  For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.


 **Baseline Settings**

The following elements are included (unlabeled GUI elements are shown in angle brackets>):







GUI Element	Description
<p><b>Baseline status</b></p>	<p>Indicates the monitor's baseline status. The following statuses are available:</p> <ul style="list-style-type: none"> <li>➤ <b>Monitor not selected for baselining.</b> The monitor has not been selected for baselining.</li> <li>➤ <b>Calculating baseline.</b> SiteScope is in the process of calculating the baseline.</li> <li>➤ <b>Calculation failed.</b> SiteScope was unable to calculate a baseline.</li> <li>➤ <b>Calculated, not activated.</b> A baseline was calculated for the monitor, but it has not yet been activated.</li> <li>➤ <b>Activating baseline.</b> SiteScope is in the process of activating the baseline.</li> <li>➤ <b>Activation failed.</b> SiteScope was unable to activate the baseline.</li> <li>➤ <b>Baseline activated.</b> The baseline has been activated for the monitor.</li> </ul> <p>The <b>Baseline mode</b> check box is selected if the baseline status is anything other than <b>Monitor not selected for baselining</b>.</p> <p>For details on using the baseline threshold, see “Setting Status Thresholds Using a Baseline” on page 312.</p>
<p><b>Remove Baseline</b></p>	<p>Click the <b>Remove Baseline</b> button to remove the baseline threshold. The baseline thresholds are removed and the static threshold value is used to create a threshold. You must remove the baseline before you can calculate the baseline after a baseline has been calculated (even if the calculation failed).</p> <p>For details on this topic, see “Setting Status Thresholds Using a Baseline” on page 312.</p>



## Dependency Dialog Box

<b>Description</b>	<p>Enables you to make the running of this monitor or monitor group dependent on the status of another monitor.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, select a monitor, and click the <b>Properties</b> tab. Expand the <b>Dependencies</b> tab, and click <b>Depends on</b> . Select the monitor on which you want to create a dependency.</p>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Monitoring Group Dependencies” on page 307</li> <li>▶ “Monitor Tree” on page 72</li> </ul>




The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
 SiteScope	Represents an individual SiteScope server.
	<p>Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors).</p> <p>If a group alert has been set up for the monitor group or subgroup, the alert  symbol is displayed next to the group icon.</p>
	<p>Represents a SiteScope monitor (enabled/disabled).</p> <p>If an alert has been set up for the monitor, the alert  symbol is displayed next to the monitor icon.</p>
	<p>Represents the collection of available health monitors that are deployed to check proper functioning of SiteScope monitors.</p> <p><b>Parent:</b> SiteScope.</p>

## Select Template Dialog Box

<b>Description</b>	<p>Enables you to select the templates you want to deploy to the monitor group.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click the group into which you want to deploy a template, and select <b>Deploy Template</b> or <b>Deploy Template Using CSV</b>.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Templates that do not contain any child objects (subgroups, monitors, variables, or a remote server) are not displayed in the template tree.</li> <li>▶ Solution templates are not displayed in the Select Template dialog box and can be deployed from the Template context only. For details, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.</li> </ul>
<b>Included in Tasks</b>	“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Updating Template Deployments” on page 1578</li> <li>▶ “SiteScope Solution Templates” on page 1665</li> <li>▶ “Monitor Tree” on page 72</li> <li>▶ “Template Tree” on page 84</li> </ul>



The following elements are included (unlabeled GUI elements are shown in angle brackets>):




<b>GUI Element</b>	<b>Description</b>
 SiteScope	Represents the SiteScope root group.
	Represents a template container. A template container is used to organize configuration deployment templates. Expand to display the templates.
	Represents a template configuration for deploying SiteScope objects. Select the templates that you want to deploy. You can select multiple templates using the CTRL or SHIFT keys.

## Copy to Template Tree Dialog Box

<b>Description</b>	<p>Enables you to copy a SiteScope object (group, monitor, or remote server) and its contents (monitors, alerts, and reports) to a template or template group.</p> <p><b>To access:</b> In the monitor or remote server tree, right-click the object you want to copy to a template, and select <b>Copy to Template</b>. In the Copy to Template dialog box, select the template or template group into which you want to copy the object.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ You can copy a group and its contents to a template provided the template does not already contain a group.</li> <li>▶ When copying a server monitor to a template, SiteScope replaces the server name with the <code>\$\$SERVER_LIST\$\$</code> variable. In this instance, we recommend creating a remote server in the template after copying the monitor to the template, and replacing the <code>\$\$SERVER_LIST\$\$</code> variable with this remote server.</li> <li>▶ The Web Script Monitor is not supported in template mode.</li> </ul>
<b>Included in Tasks</b>	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Monitor Tree” on page 72</li> <li>▶ “Template Tree” on page 84</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
 SiteScope	<p>Represents an individual SiteScope server.</p>
	<p>Represents a template container. A template container is used to organize configuration deployment templates. Template containers can hold templates only.</p>

GUI Element	Description
	<p>Represents a template configuration for deploying SiteScope objects.</p> <p>You can copy a template group (provided the template does not already contain a group), or a remote server to a template group.</p>
	<p>Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors).</p> <p>You can copy a template group or monitor to a template group.</p> <p>If a group alert has been set up for the monitor group or subgroup, the alert  symbol is displayed next to the group icon.</p>

 **Percentile Range Mapping Table**

<b>Description</b>	<p>Displays the actual value that is mapped to each percentile range. SiteScope uses the percentile value to define the baseline error and warning thresholds.</p> <p>Use this table to view the actual value that corresponds to the percentile value, and to manually change the percentile value.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, select a monitor with an activated baseline (you can check whether a monitor has an activated baseline by right-clicking a group or monitor, and select <b>Baselining &gt; Status Report</b>). Expand the monitor's <b>Threshold Settings</b>, and click the <b>Percentiles Table</b> button.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>➤ This table is available for monitors with an activated baseline only.</li> <li>➤ You can set the current percentile to a value over 100%. This enables you to raise the threshold level above the level that would have been set, based on the sample measurements collected. For example, if measurements collected for CPU Utilization are between 10%-60%, and you only want to get errors above 80% CPU Utilization, set the percentile value to a percentile that raises the error threshold level to the desired level. In this instance, set the percentile to 134% (60% CPU Utilization * 134% = 80.4% CPU Utilization).</li> </ul>
<b>Included in Tasks</b>	<p>“Set Monitor Thresholds Using a Baseline” on page 327</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Setting Status Thresholds Using a Baseline” on page 312</li> <li>➤ “Threshold Settings” on page 362</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Percentiles Range</b>	<p>The percentile range that correlates to the actual value used for defining the baseline error and warning thresholds. You can set the number of percentile ranges displayed in the table from the SiteScope Preferences (<b>Preferences &gt; Infrastructure Settings Preferences &gt; Baseline Settings</b>).</p> <p><b>Note:</b> The left-hand value is exclusive and the right-hand value is inclusive. This means that for a percentile range of 33-100, all values above 33 (but not 33 itself) up to 100 are included in the range. The value 33 falls into the previous range and 100.01 falls into the next range.</p>
<b>Actual Value</b>	The actual value that is mapped to the percentile range.
<b>Current Percentile</b>	Select a percentile value that correlates to the actual value that is used to define the baseline thresholds.

 **Calculate Baseline Dialog Box**

<b>Description</b>	<p>Use to do the following:</p> <ul style="list-style-type: none"> <li>➤ Select the groups and/or monitors to include in the baseline calculation.</li> <li>➤ Select the time range schedule for collecting baseline data.</li> <li>➤ Select and fine-tune the adherence level to determine the extent that monitor measurement sample values have on the threshold values.</li> <li>➤ Calculate the baseline threshold.</li> </ul> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope container, a group, or a monitor, and select <b>Baselining &gt; Calculate</b>.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>➤ Only an administrator in SiteScope, or a user granted <b>Edit monitors</b> permissions can use the baseline feature to set monitor thresholds, and only for the monitors that are in the users allowed groups list. Monitors in groups for which the user does not have permissions are not displayed in the dialog box.</li> <li>➤ The amount of time required to calculate the baseline thresholds depends on the speed of the SiteScope server and the number of monitors selected for baselining. If SiteScope needs to restart before the calculation process is complete, SiteScope automatically continues the process after the restart.</li> <li>➤ You should enable the monitors to run for a period that is long enough for SiteScope to accumulate sufficient data to calculate the baseline. This period depends on the <b>Minimum number of days required for baselining</b> and <b>Minimum number of samples required for baselining</b> settings in Infrastructure Settings Preferences. For details, see “Baseline Settings” on page 1408. The baseline can still be calculated and activated even if the monitor has insufficient data, although the calculation is unlikely to be accurate.</li> </ul>

<b>Included in Tasks</b>	“Set Monitor Thresholds Using a Baseline” on page 327
<b>Useful Links</b>	“Setting Status Thresholds Using a Baseline” on page 312

### Select Monitors for Baseline Calculation

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<List of available groups and/or monitors>	<p>Select the groups and/or monitors to include in calculating the baseline threshold. The list includes the currently selected container and all of the child containers that are in the users allowed groups list.</p> <p><b>Default value:</b> The current container and all child elements are selected.</p> <p><b>Note:</b> You cannot select a monitor instance if:</p> <ul style="list-style-type: none"> <li>➤ Its baseline has already been activated. In such cases, the selection check box is not displayed.</li> <li>➤ There is another monitor in SiteScope with the same name (the file path, group name, and monitor name are identical). In such cases, <b>Duplicate name</b> is displayed next to the monitor name.</li> </ul>



## Schedule

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Schedule Range Name</b>	<p>Select the schedule ranges used for collecting baseline threshold data. This enables you to restrict to certain days or hours of the week the periods during which monitor data is collected for the baseline calculation. The baseline thresholds that are created are only effective for the same schedule range period. The range schedules displayed are created in <b>Schedule Preferences</b>. For more information about creating range schedules, see “Schedule Preferences Overview” on page 1487.</p> <p><b>Note:</b> You can select multiple ranges using the CTRL or SHIFT keys.</p> <p><b>Default value:</b> If no schedule range is selected, baseline threshold data is collected all day, every day.</p>

## Adherence Level

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>Description</b>	<p>Enables you to select the adherence level that determines the extent to which monitor measurement sample values used in calculating the baseline affect the threshold values. The adherence level is based on a percentile value that is applied to all monitor measurements to determine when a measurement is in error or warning. You can also fine-tune the adherence level for individual monitor measurements, and set the Good Boundary.</p> <p><b>To access:</b> In the monitor tree, right-click the SiteScope container, a group, or a monitor, and select <b>Baselining &gt; Calculate</b>. Expand the <b>Adherence Level</b> panel.</p>
<b>Included in Tasks</b>	“Set Monitor Thresholds Using a Baseline” on page 327
<b>Useful Links</b>	“Setting the Baseline Adherence Level” on page 317

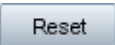

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element	Description
<b>Low adherence</b>	The further the values used to update the thresholds are from the values calculated by the baseline. Select this option if you are more tolerant to extreme measurement values having an effect on the baseline.
<b>Medium adherence</b>	The values used to update the thresholds are at a mid-range from the values calculated by the baseline (default setting).
<b>High adherence</b>	The closer the values used to update the thresholds are to the values calculated by the baseline. Select this option if you are less tolerant to extreme measurement values having an effect on the baseline.
<b>Fine-Tune Adherence Levels/Set Boundary</b>	Click to open the Fine-Tune Adherence Levels/Set Boundary dialog box. This enables you to fine-tune the baseline adherence level and define a good boundary for any measurement of any monitor type within the selected context. For details on the user interface, see “Fine-Tune Adherence Levels/Set Boundary Dialog Box” on page 387.

## Fine-Tune Adherence Levels/Set Boundary Dialog Box

<b>Description</b>	<p>Displays the percentile value used in the baseline calculation at each adherence level and the good boundary (if configured), for each monitor measurement in the selected context.</p> <p>This enables you to fine-tune the baseline adherence level and set good boundaries for any measurement of any monitor type.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope container, a group, or a monitor, and select <b>Baselining &gt; Calculate</b>. Expand the <b>Adherence Level</b> panel, and click the <b>Fine-Tune Adherence Levels/Set Boundary</b> button.</p>
<b>Important Information</b>	<p>You can set adherence level percentile values to over 100%. This enables you to raise the threshold level above the level that would have been set, based on the sample measurements collected. For example, if measurements collected for CPU Utilization are between 10%-60%, and you only want to get errors above 80% CPU Utilization, set the <b>Error Percentiles Low</b> value to a percentile that raises the error threshold level to the desired level. In this instance, set the percentile to 134% (60% CPU Utilization * 134% = 80.4% CPU Utilization).</p>
<b>Included in Tasks</b>	“Set Monitor Thresholds Using a Baseline” on page 327
<b>Useful Links</b>	“Setting Status Thresholds Using a Baseline” on page 312

The following elements are included (unlabeled GUI elements are shown in angle brackets>):




GUI Element	Description
	Click to restore the default error and warning threshold adherence level values for the monitor measurement and to remove the Good Boundary.
	Click the <b>Select All</b> button to select all listed monitor measurements.



GUI Element	Description
	Click the <b>Clear Selection</b> button to clear the selection.
<b>Monitor Name: Measurement Name</b>	For each monitor in the selected context, displays the measurements that are used in the baseline calculation. It also displays one measurement that represents the measurements for all browsable monitors (at the bottom of the list).
<b>Warning Percentiles</b>	Displays the <b>Low</b> , <b>Medium</b> , and <b>High</b> adherence level percentile value that is used to calculate the warning baseline threshold. For more details on this topic, see “Setting the Baseline Adherence Level” on page 317. <b>Default value:</b> Low 110; Medium 93; High 90
<b>Error Percentiles</b>	Displays the <b>Low</b> , <b>Medium</b> , and <b>High</b> adherence level percentile value that is used to calculate the error baseline threshold. For more details on this topic, see “Setting the Baseline Adherence Level” on page 317. <b>Default value:</b> Low 120; Medium 98; High 95
<b>Good Boundary</b>	Displays the actual value for the Good Boundary for each monitor measurement type. This is the value of a measurement that is not considered to be in error status, even though according to existing baseline percentiles it should report an error. For more details on this topic, see “Understanding the Good and Error Boundaries” on page 317. <b>Default value:</b> No value
<b>All browsable monitor measurements</b>	Displays the <b>Low</b> , <b>Medium</b> , and <b>High</b> adherence level percentile value that is used to calculate the warning and error baseline threshold for all browsable monitor measurements. <b>Default Warning values:</b> Low 110; Medium 93; High 90 <b>Default Error values:</b> Low 120; Medium 98; High 95

 **Activate Baseline Dialog Box**

<b>Description</b>	<p>Displays a summary of the calculated monitor's baseline data. For monitors that SiteScope is unable to calculate a baseline, it includes the reason for the failure.</p> <p>This dialog box enables you to:</p> <ul style="list-style-type: none"> <li>▶ Save the current monitor configuration.</li> <li>▶ View failed operations.</li> <li>▶ View baseline measurement graphs.</li> <li>▶ Activate baseline threshold configuration.</li> </ul> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a group, or a monitor and select <b>Baselining &gt; Review &amp; Activate</b>.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit monitors</b> permissions can use the baseline feature to set monitor thresholds, and only for the monitors that are in the users allowed groups list. Monitors in groups for which the user does not have permissions are not displayed in the dialog box.</li> <li>▶ To revert to the current monitor configuration, you must create a backup configuration before activating the baseline configuration.</li> <li>▶ The amount of time required to activate the baseline threshold depends on the speed of the SiteScope server and the number of monitors selected for baselining. If SiteScope needs to restart before the activation process is complete, SiteScope automatically continues the process after the restart.</li> </ul>
<b>Included in Tasks</b>	"Set Monitor Thresholds Using a Baseline" on page 327
<b>Useful Links</b>	"Setting Status Thresholds Using a Baseline" on page 312

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Successfully Calculated Monitors</b>	
	Click the <b>View Graph</b> button to display a graphical representation of baseline data for all the measurements of the monitor. For details, see “Baseline Monitor Measurement Graphs Dialog Box” on page 394.
	Click the <b>Select All</b> button to select all listed monitors.
	Click the <b>Clear Selection</b> button to clear the selection.
<b>Monitor Name</b>	The name of the SiteScope monitor selected for baselining.
<b>Calculation Date</b>	The date on which the baseline was calculated.
<b>Error Status Reduction</b>	<p>The reduction in the number of error statuses for a monitor if the baseline threshold were applied. A negative number indicates an increase in the number of error statuses for a monitor if the proposed baseline thresholds were applied.</p> <p><b>Example:</b> Suppose you manually configure the threshold status for CPU Utilization to Error if <math>\geq 65\%</math> and there are 5 error statuses for the CPU monitor (of which 3 errors are for data samples between 65%-70%, and 2 errors for above 70%). If you have SiteScope calculate the threshold using a baseline and the threshold is set to Error if <math>\geq 70\%</math>, Error Status Reduction would be 3.</p> <p><b>Note:</b> The Error Status Reduction value is based on data collected on the calculation date. If more than three days have elapsed since the calculation date, we recommend that you recalculate the baseline.</p>

GUI Element	Description
<b>Warning Status Reduction</b>	<p>The reduction in the number of warning statuses for a monitor if the baseline threshold were applied. A negative number indicates an increase in the number of warning statuses for a monitor if the proposed baseline thresholds were applied.</p> <p><b>Example:</b> Suppose you manually configure the threshold status for CPU Utilization to Warning if <math>\geq 55\%</math> and there are 3 warning statuses for the CPU monitor (of which 2 warnings are for data samples between 55%-60%, and 1 warnings for above 60%). If you have SiteScope calculate the threshold using a baseline and the threshold is set to Warning if <math>\geq 60\%</math>, Warning Status Reduction would be 2.</p> <p><b>Note:</b> The Warning Status Reduction value is based on data collected on the calculation date. If more than three days have elapsed since the calculation date, we recommend that you recalculate the baseline.</p>
<b>Failed Monitors</b>	
	Click the <b>Select All</b> button to select all listed failed monitors.
	Click the <b>Clear Selection</b> button to clear the selection.
<b>Monitor Name</b>	The name of the monitor for which SiteScope was unable to calculate a baseline.

GUI Element	Description
<p><b>Reason for Failure</b></p>	<p>The reason that SiteScope was unable to calculate a baseline value for the monitor. They include:</p> <ul style="list-style-type: none"> <li>▶ <b>Insufficient data.</b> The monitor has not run for a sufficient period of time to collect data to produce a meaningful baseline threshold. This period depends on the <b>Minimum number of days required for baselining</b> and <b>Minimum number of samples required for baselining</b> settings in Infrastructure Settings Preferences. For details on configuring the Baseline Settings, see “Baseline Settings” on page 1408.</li> <li>▶ <b>No measurements to baseline.</b> The monitor has no measurements that can be used in the baseline calculation. You cannot select the monitor for baseline activation.</li> <li>▶ <b>No samples for the requested schedule.</b> No data samples were collected for the range schedule specified. You cannot select the monitor for baseline activation.</li> <li>▶ <b>Unknown.</b> The reason for baseline calculation failure is unknown. You cannot select the monitor for baseline activation.</li> </ul>
<p><b>Can Be Activated</b></p>	<p>Indicates whether a baseline can be activated even if the monitor baseline calculation failed.</p> <p>Displays <b>No</b> if the baseline calculation failed for any reason other than <b>Insufficient data</b>.</p> <p>Displays <b>Yes</b> if the baseline calculation failed with the reason <b>Insufficient data</b>. SiteScope uses the limited measurement samples that were collected to calculate the baseline.</p>



## Backup Configuration Dialog Box

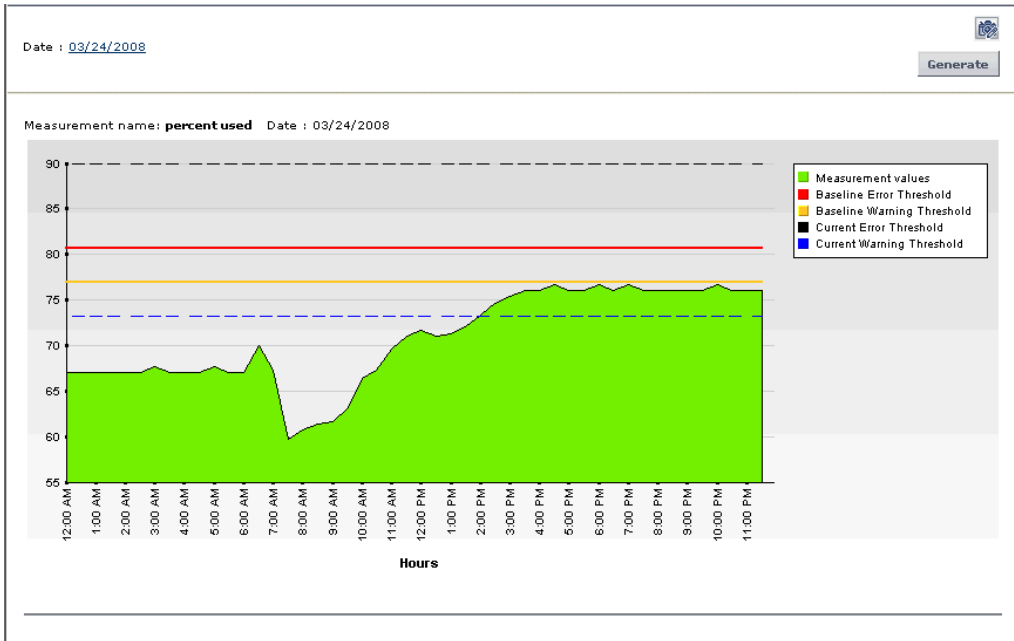
<b>Description</b>	<p>Enables you to save the current monitor threshold configuration before activating the baseline threshold. You use the Configuration Tool to restore the configuration settings. For details on the Configuration Tool, refer to the <i>HP SiteScope Deployment Guide</i> PDF.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a group, or a monitor and select <b>Baselining &gt; Review &amp; Activate</b>. Click the <b>Backup Configuration</b> button.</p>
<b>Important Information</b>	Create a backup configuration before activating the baseline configuration, since you cannot undo threshold configuration changes after the baseline has been activated.
<b>Included in Tasks</b>	“Set Monitor Thresholds Using a Baseline” on page 327
<b>Useful Links</b>	“Setting Status Thresholds Using a Baseline” on page 312

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Enter target directory</b>	<p>Enter the target directory where the backup configuration file is saved or use the default SiteScope installation directory.</p> <p><b>Default value:</b> C:\SiteScope</p>
<b>Enter the backup file name</b>	<p>Enter a name for the configuration backup file. By default, the file is named using the format: SiteScope_&lt;MM_DD_YYYY&gt;_&lt;HH_MM_SS&gt;. SiteScope saves a backup file in zip format to the specified location.</p> <p><b>Example:</b> SiteScope__11_05_2008_08_24_06</p>

## **Baseline Monitor Measurement Graphs Dialog Box**


The following is an example of a Baseline Monitor Measurement graph.



<b>Description</b>	<p>Displays a graph per measurement, for all the measurements of the monitor. The default date selected for displaying the graph is the day with the maximum error reduction.</p> <p>Each graph shows:</p> <ul style="list-style-type: none"> <li>▶ The current warning and error thresholds.</li> <li>▶ The baseline warning and error thresholds.</li> <li>▶ Historic data of all baseline-related monitor measurements over a 24-hour time period (from 00:00-23:59).</li> </ul> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a group or a monitor container, and select <b>Baselining &gt; Review &amp; Activate</b>. In the <b>Select Monitors for Baseline Activation</b> panel, select a monitor with calculated baseline data, and click the <b>View Graph</b> button.</p>
<b>Important Information</b>	<p>The data displayed in the monitor measurement graphs is an aggregate of the measurement data and as such, the time periods may not accurately reflect the time the data was actually collected.</p>
<b>Included in Tasks</b>	<p>“Set Monitor Thresholds Using a Baseline” on page 327</p>
<b>Useful Links</b>	<p>“Setting Status Thresholds Using a Baseline” on page 312</p>

## Graph Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click to create a snapshot of the graph you are viewing and highlight important areas of the graph by drawing shapes, lines, and adding text to the snapshot. For details on the user interface, see “Annotation Tool” on page 2085.
<b>Historic date &lt;date link&gt;</b>	Click the date link to open the calendar, and select the date for which you want to create monitor measurement graphs. The calendar contains the following buttons: <ul style="list-style-type: none"> <li>➤ <b>Revert.</b> Returns to the previously selected report date.</li> <li>➤ <b>Current.</b> Selects today’s date in the calendar.</li> <li>➤ <b>OK.</b> Updates the date link for the selected date and closes the calendar.</li> <li>➤ <b>Cancel.</b> Closes the calendar without making any changes.</li> </ul>
<b>Generate</b>	Click to create a report for the date displayed in the date link.

## Graph Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Legend>	Describes the color coding used in the graph.
Measurement name	The name of the measurement appears above the graph.
Date	The time and date on which the graph was generated.
<Data points>	Displays for each 2 hour period of time on the <b>Time</b> axis, the value for the selected monitor measurement. <b>Tooltip:</b> The measurement value.
<Measurement Type> <y-axis>	Displays the monitor measurement type.
Time <x-axis>	The time division units for the date specified when generating the report (from 0-24 hours).
Baseline Error Threshold	Shows the baseline threshold line that determines <b>Error</b> status. Measurements beyond this line exceed the error baseline status threshold for the monitor. This is displayed on the graph as a solid red line.
Baseline Warning Threshold	Shows the baseline threshold line that determines <b>Warning</b> status. Measurements beyond this line exceed the warning baseline status threshold for the monitor. This is displayed on the graph as a solid orange line.
Current Error Threshold	Shows the threshold line that determines <b>Error</b> status. Measurements beyond this line exceed the error status threshold for the monitor. This is displayed on the graph as a dashed black line.
Current Warning Threshold	Shows the threshold line that determines <b>Warning</b> status. Measurements beyond this line exceed the warning status threshold for the monitor. This is displayed on the graph as a dashed blue line.

## Remove Baseline Dialog Box

<b>Description</b>	<p>Enables you to select the groups and/or monitors from which to remove the baseline. You must remove a monitor's existing baseline calculation before you can recalculate the monitor's threshold baseline.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a group, or a monitor and select <b>Baselining &gt; Remove</b>.</p>
<b>Important Information</b>	<p>Only an administrator in SiteScope, or a user granted <b>Edit monitors</b> permissions can remove a baseline, and only for the monitors that are in the users allowed groups list. Monitors in groups for which the user does not have permissions are not displayed in the dialog box.</p>
<b>Included in Tasks</b>	"Set Monitor Thresholds Using a Baseline" on page 327
<b>Useful Links</b>	"Setting Status Thresholds Using a Baseline" on page 312

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<List of groups and/or monitors>	<p>Select the groups and/or monitors from which you want to remove baseline threshold calculation. The list includes all groups and/or monitors in the currently selected container and all of the child containers that are in the users allowed groups list.</p> <p><b>Default value:</b> The current container and all child elements are selected.</p>

## Baseline Status Report

The following is an example of the Baseline Status Report.

Baseline Status Report			
Summary			
<p><b>Total of 10 monitors.</b>  <b>2 monitors have an activated baseline.</b>  <b>The calculation failed for 1 monitor.</b>  <b>7 monitors are not baselined.</b></p>			
Details			
Monitor Name	Monitor Type	Baseline Status	Baseline Status Details
SiteScope\AutoSanity\Basic\Disabl...	CPU	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\CPU U...	CPU	Baseline activated	
SiteScope\AutoSanity\Basic\Memo...	Memory	Calculation failed	No measurements to baseline
SiteScope\AutoSanity\Basic\FTP o...	Port	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\URL L...	URL List	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\Disk S...	Disk Space	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\Direct...	Directory	Baseline activated	
SiteScope\AutoSanity\Basic\Link C...	Link Check	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\ Servi...	Service	Monitor not selected for baselining	
SiteScope\AutoSanity\ddd:ddd	CPU	Monitor not selected for baselining	

<b>Description</b>	<p>Displays information about the baseline status for all monitors in the selected context.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a group, or a monitor and select <b>Baselining &gt; Status Report</b>.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This is an ad hoc report that is not saved to the SiteScope configuration data for later use.</li> <li>▶ You can sort monitor types in ascending or descending order by clicking the column header. An arrow is displayed showing the sort order direction.</li> <li>▶ You can filter the display for Monitor Type and Baseline Status by clicking the down arrow ▾ and selecting a monitor type or baseline status by which to filter. To clear the filter, select <b>(All)</b>.</li> </ul>
<b>Included in Tasks</b>	“Set Monitor Thresholds Using a Baseline” on page 327
<b>Useful Links</b>	“Setting Status Thresholds Using a Baseline” on page 312

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Monitor Name</b>	<p>The name and path of the SiteScope monitor depending on the context.</p> <p><b>Note:</b> Only monitors in groups or subgroups that a user has permissions to access are displayed in the report.</p>
<b>Monitor Type</b>	<p>The type of SiteScope monitor.</p>
<b>Baseline Status</b>	<p>The monitor's baseline status. The following statuses are available:</p> <ul style="list-style-type: none"> <li>➤ <b>Monitor not selected for baselining.</b> The monitor has not been selected for baselining.</li> <li>➤ <b>Calculating baseline.</b> SiteScope is in the process of calculating the baseline.</li> <li>➤ <b>Calculation failed.</b> SiteScope was unable to calculate a baseline.</li> <li>➤ <b>Calculated, not activated.</b> A baseline was calculated for the monitor, but it has not yet been activated.</li> <li>➤ <b>Activating baseline.</b> SiteScope is in the process of activating the baseline.</li> <li>➤ <b>Activation failed.</b> SiteScope was unable to activate the baseline.</li> <li>➤ <b>Baseline activated.</b> The baseline has been activated for the monitor.</li> </ul>



GUI Element	Description
<b>Baseline Status Details</b>	<p>Displays additional details for monitors with the following status:</p> <ul style="list-style-type: none"> <li>▶ <b>Calculating baseline.</b> Displays the baseline calculation stage for the monitor.</li> <li>▶ <b>Calculation failed.</b> Displays the reason that the baseline calculation failed (<b>Insufficient data, No measurements to baseline</b>). Monitors that failed due to insufficient data are selected by default for automatic baseline calculation after the monitors have run for a period that is sufficient for SiteScope to accumulate data for the baseline period. For details, see “Activate Baseline Dialog Box” on page 389.</li> </ul>
<b>Refresh</b>	Click the <b>Refresh</b> button during the calculation process to update the data in the status report.



# 11

---

## Monitoring XML Documents

This chapter includes concepts and reference information about SiteScope's content matching capabilities for XML documents.

### **This chapter includes:**

#### Concepts

- ▶ Monitoring XML Documents Overview on page 403

#### Reference

- ▶ Content Matching for XML Documents on page 404
- ▶ Using XML Content Match Values in Monitor Configurations on page 406

### **Monitoring XML Documents Overview**

SiteScope's content matching capabilities is an important function in monitoring networked information systems and content. For SiteScope monitors that provide content matching, the basic content matching is available through the use of Perl regular expressions. SiteScope also includes the capability of matching document content by traversing XML documents. For example, you can include an XML match content string using the URL Monitor and Web Services Monitor to match an XML element name, an attribute of an XML element, or the content of an element. You can use this to check for content in XML based Web pages, SOAP or XML-RPC documents, and even WML pages served to WAP-enabled devices.

## Content Matching for XML Documents

The syntax of XML match content strings reflects the hierarchal structure of the XML document. Match content strings that start with "xml" are recognized as element names within an XML document. The element names are added, separated by periods, in the order of their relationship to the root element. For example, in the document `weather.xml` the root element is `<weather>`. This element includes child elements named `<area>`, `<skies>`, `<wind>`, `<forecast>`, and so forth. To access the content of these XML elements or their attributes, you would use a syntax like `xml.weather.area`.

To check that specific content or value is present, add an equals sign after the element name whose content you are testing and then add the value of the content. If there are multiple instances of an element name in the document, you can check a particular instance of that element by adding the number indicating the order of the element in the document in square brackets (see the example in the table below). You can also test for multiple elements or values by separating individual search strings with commas. The table below gives several examples of the syntax used to match content in XML documents.

Example Match Content	Description
xml.weather.temperature	Succeeds if any <code>&lt;weather&gt;</code> node in the document contains <b>one or more</b> <code>&lt;temperature&gt;</code> elements. The content of the <code>&lt;temperature&gt;</code> elements is returned by the monitor. If no <code>&lt;temperature&gt;</code> element is found within the <code>&lt;weather&gt;</code> node, an error is returned.
xml.weather.temperature=20	Succeeds if any <code>&lt;weather&gt;</code> node in the document contains <b>one or more</b> <code>&lt;temperature&gt;</code> elements where the content of the <code>&lt;temperature&gt;</code> element equals 20. The content of the <code>&lt;temperature&gt;</code> element is <b>not</b> returned by the monitor if the match is found. An error is returned if no <code>&lt;temperature&gt;</code> element is found within the <code>&lt;weather&gt;</code> node or if no <code>&lt;temperature&gt;</code> element contains the value 20.

Example Match Content	Description
xml.weather.forecast.[confidence]	Succeeds if any <weather> node in the document contains a <forecast> element that has an <b>attribute</b> called confidence. The value of the confidence attribute is returned by the monitor if the match is found. An error is returned if no <forecast> element is found within the <weather> node or if no confidence attribute is found.
xml.weather.forecast[3].[confidence]=50	Succeeds if any <weather> node in the document contains three or more <forecast> elements where the third <forecast> element has a confidence <b>attribute</b> with a value of 50. An error is returned if the <weather> node has fewer than three <forecast> elements or if the value of the confidence attribute is not equal to 50.
xml.weather.temperature=20, xml.weather.skies=rain	Succeeds if any <weather> node in the document contains <b>one or more</b> <temperature> elements where the content of the <temperature> element equals 20 <b>and</b> if any <weather> node contains <b>one or more</b> <skies> elements where the content of the <skies> element equals rain. Returns an error if either of the matches fails.
xml.wml.card.p.table.tr.td.anchor=Home Page	Checks the content of <anchor> elements in the designated path of a WML document. Succeeds if any <card> node containing table cells with <b>one or more</b> <anchor> elements where the content of any of the <anchor> elements equals "Home Page."

## Using XML Content Match Values in Monitor Configurations

Monitors like the URL Monitor have a content match value that is logged to the SiteScope monitor data log and can also be used to set error and warning status thresholds for the monitor. The values of the XML names are saved as the content match values for the monitor.

For example, if the match content expression was `xml.weather.temperature` and the document was the contents of the file `weather.xml`, then the content match value would be 46.

You can then set the error, warning, and good status thresholds in the Advanced Options section for the monitor to compare your specific thresholds to the value returned by the content match.

For example, if you were monitoring temperature values and wanted to be alerted when the temperature value dropped below 72 degrees, you could set the monitor status thresholds as follows:

<b>Error if</b>	<code>content match &lt; &lt;= 72</code>
<b>Warning if</b>	<code>content match == &lt;= 72</code>
<b>Good if</b>	<code>content match &gt;= &gt; 72</code>

With this configuration, the monitor would check the content of the temperature element and then compare it to the error and warning thresholds. In the example above, the status of the monitor would be **error** because the temperature value is 46, which is less than 72.

# 12

---

## Active Directory Replication Monitor

This chapter includes the main concepts and reference information for the Active Directory Replication monitor.

### **This chapter includes:**

#### Concepts

- ▶ Active Directory Replication Monitor Overview on page 407

#### Reference

- ▶ Active Directory Replication Monitor Settings on page 409

### **Active Directory Replication Monitor Overview**

Use the Active Directory Replication monitor to monitor the time that it takes a change made on one Domain Controller to replicate to up to as many as ten other Domain Controller. This enables you to verify that replication, a key part of the Active Directory System, is occurring within set thresholds. Create a separate Active Directory Replication monitor for each Domain Controller that is being replicated throughout your system.

This monitor supports monitoring remote servers running on Windows Server 2000 and Windows Server 2003.

**Note:**

- ▶ The Active Directory Replication monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
  - ▶ This monitor can only be added by deploying an Active Directory Solution template. For information about using templates to deploy monitors, see “SiteScope Templates” on page 1557.
- 

No additional setup is required other than to enable access to a Domain Admin account.

The Active Directory Replication monitor works by making a small change to part of the Directory Service tree of the configured Domain Controller. It then checks each of the configured Replicating Domain Controllers for this small change. As the change is detected the difference between when the change was made and when it was replicated is calculated.

For details on configuring the monitor, see “Active Directory Replication Monitor Settings” on page 409.



## Active Directory Replication Monitor Settings

<p><b>Description</b></p>	<p>The Active Directory Replication monitor enables you to monitor the time that it takes replication to occur between up to ten Domain Controllers. The error and warning thresholds for the monitor can be set on each of the monitored Domain Controllers.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Templates</b> context. In the template tree, expand the <b>Solution Templates</b> container. Right-click the Active Directory solution template that you require, and select <b>Deploy Template</b>. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ This monitor can only be added by deploying an Active Directory Solution template. For information about using templates to deploy monitors, see "SiteScope Templates" on page 1557.</li> <li>▶ The <b>LDAP Authentication Tool</b> is available when configuring this monitor to authenticate a user on an LDAP server (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see "LDAP Authentication Tool" on page 211.</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ "Active Directory Replication Monitor Overview" on page 407</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 354.</li> </ul>

## Active Directory Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Domain controller</b>	Select the domain controller that contains the replicated data.
<b>Replicating domain controllers</b>	Enter a comma separated list of domain controllers that replicate data from the domain controller entered above.
<b>User name</b>	<p>Enter either the user name or the entire Security Principal of a Domain Admin account.</p> <p>If a user name is given, the default security principal is created from the root context of the Domain Controller.</p> <p><b>Example:</b> If you enter Administrator for a domain controller in the domain yourcompany.com, then the entire Security Principal would be CN=Administrator,CN=Users,DC=yourcompany,DC=com.</p>
<b>Password</b>	Enter the password for the Domain Admin account.
<b>Maximum replication time (seconds)</b>	<p>Enter the maximum amount of time for replication to occur. The monitor goes into error if any of the Replicating Domain Controllers exceed this replication time.</p> <p><b>Default value:</b> 600 seconds</p>
<b>Polling interval (seconds)</b>	<p>The amount of time this monitor should wait between queries of the Replicating Domain Controllers. A higher number reduces the number of LDAP queries against the servers.</p> <p><b>Default value:</b> 10 seconds</p>
<b>Directory path</b>	<p>The path to a directory in the Active Directory that you want to monitor. This is in the form of an LDAP query.</p> <p><b>Default value:</b> Based on the default Directory for this server. For example, the default for a Domain Controller for sub.yourcompany.com is DC=sub,DC=yourcompany,DC=com.</p>

# 13

---

## Apache Server Monitor

This chapter includes the main concepts and reference information for the Apache Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ Apache Server Monitor Overview on page 411

#### Reference

- ▶ Apache Server Monitor Settings on page 413

### **Apache Server Monitor Overview**

Use the Apache Server monitor to monitor the content of server administration pages for Apache 1.3.9, 1.3.12, 2.0 and 2.2 servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Apache server you are running.

This section also includes:

- ▶ “Setup Requirements and User Permissions” on page 412
- ▶ “Configuring the Monitor” on page 412

## Setup Requirements and User Permissions

Before you can use the Apache Server monitor, you must do the following:

- ▶ Configure the Apache server you want to monitor so that status reports (server-status) are enabled for the server. The steps needed to do this may vary depending on the version of Apache you are using.
- ▶ Enable extended status (ExtendedStatus On) in the configuration file.
- ▶ Know the URL of the server statistics page for the server you want to monitor.
- ▶ Know the user name and password for accessing the counters of the Apache server you want to monitor, if required.
- ▶ If using a proxy server to access the server, get the domain name and port of an HTTP Proxy Server from your network administrator.
- ▶ The SiteScope Apache Server monitor currently supports the server status page available at `http://<server_address>:<port>/server-status?auto`. The port is normally port 80, although this may vary depending on the server set up and your environment. For some Apache server configurations, you may need to use the server name rather than an IP address to access the server statistics page.

## Configuring the Monitor

For details on configuring the monitor, see “Apache Server Monitor Settings” on page 413.

## Apache Server Monitor Settings

<b>Description</b>	<p>Use to monitor the administrative and performance statistics for an Apache server.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Apache Server Monitor Overview” on page 411</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### Apache Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server Settings</b>	
<b>Administration URL</b>	Choose the server URL you want to verify with this monitor. This should be the Apache server statistics URL which usually has the form of <code>http://&lt;servername&gt;:&lt;port&gt;/server-status?auto</code> .
<b>Operating System</b>	The operating system that the Apache server is running on. This is used to correctly read server statistics from Apache based on the operating system platform. <b>Default value:</b> UNIX
<b>Counter Settings</b>	

GUI Element	Description
<b>Counters</b>	Select the server performance counters you want to check with this monitor. The list displays the available counters and those currently selected for this monitor.
<b>Connection Settings</b>	
<b>Authorization user name</b>	If the server you want to monitor requires a name and password for access, enter the name.
<b>Authorization password</b>	If the server you want to monitor requires a name and password for access, enter the password.
<b>HTTP Proxy</b>	(Optional) A proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.
<b>Proxy user name</b>	If the proxy server requires a name and password to access the server, enter the name here. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy password</b>	If the proxy server requires a name and password to access the server, enter the password here. <b>Note:</b> your proxy server must support Proxy-Authenticate for these options to function.
<b>Timeout (seconds)</b>	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status. <b>Default value:</b> 60 seconds

# 14

---

## BroadVision Application Server Monitor

This chapter includes the main concepts and reference information for the BroadVision Application Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ BroadVision Application Server Monitor Overview on page 415

#### Reference

- ▶ BroadVision Application Server Monitor Settings on page 416

### **BroadVision Application Server Monitor Overview**

Use the BroadVision Application Server monitor to monitor the server performance data for BroadVision 4.1, 5.x, and 6.0 servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each BroadVision server in your environment.

This section also includes:

- ▶ “Setup Requirements:” on page 416
- ▶ “Configuring the Monitor” on page 416

### Setup Requirements:

The following are important requirements for using the BroadVision Application Server monitor:

- ▶ You must know the Object Request Broker (ORB) port number for the BroadVision server you are trying to monitor.
- ▶ In a BroadVision Production-style environment where there is one primary root server and other secondary servers (for example, Interaction Manager node) on different machines, you can only define a monitor against the primary root node. Metrics for the other nodes in the configuration are available for selection during root node monitor definition. In other words, monitoring is always accomplished through the primary root node, for all servers.

### Configuring the Monitor

For details on configuring the monitor, see “BroadVision Application Server Monitor Settings” on page 416.

## BroadVision Application Server Monitor Settings

<p><b>Description</b></p>	<p>Monitor the availability and performance statistics of a BroadVision server. The error and warning thresholds for the monitor can be set on one or more BroadVision server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>



<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “BroadVision Application Server Monitor Overview” on page 415</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## BroadVision Application Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>Server</b>	Enter the BroadVision root server name of the BroadVision server you want to monitor. For example, 199.123.45.678.
<b>Port</b>	Enter the ORB port number to the BroadVision server you want to monitor. <b>Example:</b> 1221
<b>Counter Settings</b>	
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor. <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.



# 15

---

## Browsable Windows Performance Monitor

This chapter includes the main concepts and reference information for the Browsable Windows Performance monitor.

### **This chapter includes:**

#### Concepts

- ▶ Browsable Windows Performance Counter Monitor Overview on page 419

#### Reference

- ▶ Browsable Windows Performance Counter Monitor Settings on page 421

### **Browsable Windows Performance Counter Monitor Overview**

Use the Browsable Windows Performance Counter monitor to monitor the values of Windows performance statistics. Each time the Browsable Windows Performance Counter monitor runs, it returns readings and a status message and writes them in the monitoring log file. The status is displayed in the group detail table for the monitor which represents the current value returned by this monitor. The status is logged as either OK or warning. A count of the number of counters that could not be read is also kept, and error conditions can be created depending on this count.

**Note:**

- ▶ The Browsable Windows Performance Counter monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
  - ▶ This monitor can be added only by deploying a Microsoft Exchange Solution Template. For information about using templates to deploy monitors, see “SiteScope Solution Templates” on page 1665.
  - ▶ This monitor is supported in SiteScopes that are running on Windows versions only.
- 

For details on configuring the monitor, see “Browsable Windows Performance Counter Monitor Settings” on page 421.

## **Browsable Windows Performance Counter Monitor Settings**

<p><b>Description</b></p>	<p>The Browsable Windows Performance Counter monitor tracks the values of Windows performance statistics. These are the same statistics that can be viewed using the Performance monitor application under Windows.</p> <p>This monitor is only available on the Windows version of SiteScope.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Templates</b> context. In the template tree, expand the <b>Solution Templates</b> container. Right-click the required Microsoft Exchange Solution Template, and select <b>Deploy Template</b>. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ This monitor can only be added by deploying a Microsoft Exchange Solution Template. For more information, see “SiteScope Solution Templates” on page 1665. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Browsable Windows Performance Counter Monitor Overview” on page 419</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Browsable Windows Performance Counter Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Server</b>	<p>Enter the server where the performance counters you want to monitor are found.</p> <p><b>Note:</b> After deployment, you can use the drop-down list to select a server from the list of Microsoft Windows remote servers that are available to SiteScope.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p>
<b>Counter file</b>	<p>The file that contains a list of counters from which to choose to monitor. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.</p> <p>The files in this list all reside in the <code>&lt;SiteScope root directory&gt;\templates.perfmon\browsable</code> directory under SiteScope. There are a number of default files in the standard SiteScope distribution.</p>

GUI Element	Description
<b>Counters</b>	<p>The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p><b>Note when working in template mode:</b> To update counters in template browsable monitors that need a target server, click the <b>Select measurement from</b> button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the <b>Server</b> field.</p>
<b>Get Counters</b>	<p>Click to open the Select Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>





# 16

---

## Check Point Monitor

This chapter includes the main concepts and reference information for the Check Point monitor.

**This chapter includes:**

**Concepts**

- ▶ Check Point Monitor Overview on page 426

**Reference**

- ▶ Check Point Monitor Settings on page 426

## Check Point Monitor Overview

Use the Check Point monitor to monitor the content of event logs and other data from Check Point Firewall-1 4.1 NG servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate Check Point monitor instance for each Check Point Firewall-1 server in your environment.

For details on configuring the monitor, see “Check Point Monitor Settings” on page 426.

## Check Point Monitor Settings

<b>Description</b>	<p>Monitor the statistics of a Check Point Firewall-1 server using SNMP. The error and warning thresholds for the monitor can be set on one or more firewall statistics.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Check Point Monitor Overview” on page 426</li> <li>➤ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Check Point Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Main Settings</b>	
<b>Index</b>	Enter the index of the SNMP object you want to check with this monitor. Non-table object IDs have an index of 0 (zero). <b>Default value:</b> 0
<b>Community</b>	Enter the community name of the Check Point Firewall-1 you want to monitor. You may need to consult with your network administrators about what community names are active in your network environment. <b>Default value:</b> public
<b>Host</b>	Enter the host name or IP address of the Check Point Firewall-1 server you want to monitor. If the Check Point Firewall is configured to respond to SNMP on a port number other than the default port (161), enter the port number as part of the server address.
<b>Retry delay (seconds)</b>	The number of seconds that the monitor should wait for a response from the server before retrying the request. <b>Default value:</b> 1 second
<b>Timeout (seconds)</b>	The number of seconds that the monitor should wait for a response from the server before timing out. Once this time period passes, the monitor logs an error and reports an error status. <b>Default value:</b> 5 seconds
<b>Counter Settings</b>	
<List of counters>	Displays the available server performance counters and those currently selected for this monitor.



# 17

---

## Cisco Works Monitor

This chapter includes the main concepts and reference information for the Cisco Works monitor.

### **This chapter includes:**

#### Concepts

- ▶ Cisco Works Monitor Overview on page 429

#### Reference

- ▶ Cisco Works Monitor Settings on page 430

### **Cisco Works Monitor Overview**

Use the Cisco Works monitor to monitor the content of event logs and other data from Cisco Works 2000 servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate Cisco Works monitor instance for each Cisco Works server in your environment.

For details on configuring the monitor, see “Cisco Works Monitor Settings” on page 430.



## Cisco Works Monitor Settings

<b>Description</b>	<p>Monitor the statistics of a Cisco Works Server using SNMP. The error and warning thresholds for the monitor can be set on one or more Cisco Works server statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ The <b>SNMP Browser Tool</b> is available when configuring this monitor to verify the connection properties of an SNMP agent and to gain more information about the MIBs which that agent implements (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “SNMP Browser Tool” on page 237.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Cisco Works Monitor Overview” on page 429</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Cisco Works Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>SNMP Connection Settings</b>	
<b>Server</b>	Enter the name of the server you want to monitor.
<b>SNMP version</b>	Select the version of SNMP to use when connecting. Supports SNMP version 1, 2, and 3. Selecting V3 enables you to enter V3 settings in the SNMP V3 settings panel. <b>Default value:</b> V1
<b>Community</b>	Enter the community name of the Cisco Works Server you want to monitor (valid only for version 1 or 2 connections). You may need to consult with your network administrators about what community names are active in your network environment. <b>Default value:</b> public
<b>Timeout (seconds)</b>	Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. <b>Default value:</b> 5
<b>Retries</b>	Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. <b>Default value:</b> 1
<b>Port</b>	Enter the port to use when requesting data from the SNMP agent. <b>Default value:</b> 161

GUI Element	Description
<b>Starting OID</b>	<p>Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered here. You should edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value of 1 did not enable retrieving any counters, then you may have to enter a different value.</p> <p><b>Default value:</b> 1</p>
<b>MIB file</b>	<p>Select either the <b>CISCOWORKS-MIB.my</b> file or <b>All MIBs</b>. Selecting the <b>CISCOWORKS-MIB.my</b> file causes only those objects that are described within that MIB file to be displayed.</p> <p>Selecting <b>All MIBs</b> causes all objects discovered on the given Cisco Works server to be displayed when browsing counters.</p> <p>If no MIB information is available for an object, it is still displayed, but with no textual name or description.</p> <p><b>Default value:</b> All MIBs</p>
<b>Counter calculation mode</b>	<p>Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are:</p> <ul style="list-style-type: none"> <li>▶ <b>Calculate delta.</b> Calculates a simple delta of the current value from the previous value.</li> <li>▶ <b>Calculate rate.</b> Calculates a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements.</li> <li>▶ <b>Do not calculate.</b> No calculation is performed.</li> </ul> <p><b>Note:</b> This option only applies to the aforementioned object types. A Cisco Works monitor that monitors Counter objects as well as DisplayString objects only performs this calculation on the Counter objects.</p>
<p><b>V3 SNMP Settings</b> (This panel is enabled only if V3 is selected in the SNMP version field)</p>	



GUI Element	Description
<b>SNMP V3 authentication type</b>	Select the type of authentication to use for version 3 connections. <b>Default value:</b> MD5
<b>SNMP V3 user name</b>	Enter the user name for version 3 connections.
<b>SNMP V3 authentication password</b>	Enter the authentication password to use for version 3 connections.
<b>SNMP V3 privacy password</b>	Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.
<b>SNMP V3 context engine ID</b>	Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.
<b>SNMP V3 context name</b>	Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.
<b>SNMP Counters</b>	

GUI Element	Description
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ The counters displayed are those received during the timeout period, and may not include all the counters available on the server. Specifying a longer timeout in the Timeout (seconds) field in the SNMP Connection Settings panel may result in receiving more counters.</li> <li>▶ The total time for receiving the counters may be longer than the timeout specified, due to additional processing time not part of the request/response period.</li> <li>▶ Due to third-party counter restrictions, the total number of counters that can be monitored is limited to 32.</li> </ul> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

# 18

---

## Citrix Monitor

This chapter includes the main concepts and reference information for the Citrix monitor.

### **This chapter includes:**

#### Concepts

- ▶ Citrix Monitor Overview on page 435

#### Reference

- ▶ Citrix Monitor Settings on page 439

### **Citrix Monitor Overview**

Use the Citrix monitor to monitor the server performance statistics from Citrix servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate Citrix monitor instance for each Citrix server in your environment.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only. Target server must also be running on Windows platform.

---

The Citrix monitor makes use of performance objects and counters to measure application server performance. The Citrix monitor keeps track of the following performance objects:

- ▶ Citrix IMA Networking
- ▶ Citrix Presentation Server (Citrix MetaFrame XP)
- ▶ ICA Session
- ▶ Terminal Services Session

You can find information about the Citrix performance objects and their counters in Appendix C of the Presentation Server 4.0 Administrator's Guide (<http://support.citrix.com/article/CTX106319>), and about the Terminal Services Session Object at

<http://technet2.microsoft.com/windowsserver/en/library/9784cf82-9d06-4efa-b6fc-51c803fe78671033.mspx?mfr=true>.

This section also includes:

- ▶ “Supported Versions” on page 436
- ▶ “Setup Requirements and User Permissions” on page 437
- ▶ “Troubleshooting and Limitations” on page 437
- ▶ “Configuring the Monitor” on page 438

### **Supported Versions**

This monitor supports monitoring remote servers running on:

- ▶ Citrix MetaFrame 1.8 Service Pack 3
- ▶ Citrix MetaFrame XP(s,a,e) Feature Release 1/Service Pack 1
- ▶ Citrix MetaFrame XP(s,a,e) Feature Release 2/Service Pack 2
- ▶ Citrix Presentation Server 3.5
- ▶ Citrix Presentation Server 4.x

## Setup Requirements and User Permissions

The following are important requirements for using the SiteScope Citrix monitor:

- ▶ SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you must define the connection to these servers under the Microsoft Windows Remote Servers option in Remote Servers.
- ▶ The Remote Registry service must be running on the machine where the Citrix is running if Citrix is running on a Windows 2000 platform.
- ▶ The Citrix Resource Manager must be available, installed, and running on the Citrix servers you want to monitor.
- ▶ One or more Citrix vusers must have established a connection with the Citrix server to enable viewing of ICA Session object.
- ▶ The Citrix monitor requires the same permissions (trust level between monitoring and monitored machines) in Windows 2003 as Microsoft Windows Resources monitor. For details, see “Configuring the Monitor to Run on Windows 2003 as a Non-Administrator User” on page 716.

## Troubleshooting and Limitations

Perform the following steps to troubleshoot the Citrix monitor.

**To troubleshoot the Citrix monitor:**

- 1** Open a command line window (DOS prompt).
- 2** Enter the following command, substituting the host name as required:

```
C:\>perfex \\hostname -u username -p password -h | find "ICA"
```

**3** This should return the following response:

```
(3378) ICA Session  
(3386) ICA Session  
(3379) This object has several counters that can be used to monitor the performance in  
ICA sessions  
(3387) This object has several counters that can be used to monitor the performance in  
ICA sessions"  
ICA Session" 3386 performance in ICA sessions
```

If you do not get a similar response, either the counters are not available on the remote server or you a more descriptive error message is displayed indicating what might be the problem.

### **Configuring the Monitor**

For details on configuring the monitor, see “Citrix Monitor Settings” on page 439.

 **Citrix Monitor Settings**

<b>Description</b>	<p>Monitor the availability of the Citrix Presentation (MetaFrame) server. The error and warning thresholds for the monitor can be set on one or more Citrix server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Citrix Monitor Overview” on page 435</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Citrix Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the Citrix server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>



GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>
<b>Counters</b>	<p>The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters. For information about the Citrix performance counters, see Appendix C of the MetaFrame Presentation Server 4.0 Administrator's Guide (<a href="http://support.citrix.com/article/CTX106319">http://support.citrix.com/article/CTX106319</a>).</p> <p><b>Note when working in template mode:</b> To update counters in template browsable monitors that need a target server, click the <b>Select measurement from</b> button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the <b>Server</b> field.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p>



# 19

---

## ColdFusion Server Monitor

This chapter includes the main concepts and reference information for the ColdFusion Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ ColdFusion Server Monitor Overview on page 443

#### Reference

- ▶ ColdFusion Server Monitor Settings on page 445

### **ColdFusion Server Monitor Overview**

Use the ColdFusion Server monitor to monitor the server performance statistics from ColdFusion 4.5.x servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate ColdFusion Server monitor instance for each ColdFusion server in your environment.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only.

---

This section also includes:

- “Setup Requirements” on page 444
- “Configuring the Monitor” on page 444

## **Setup Requirements**

The following are important requirements for using the ColdFusion Server monitor:

- The ColdFusion Server monitor makes use of performance counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you must define the connection to these servers in the Microsoft Windows Remote Servers container. For details on how to define the Windows server connection, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
- The Remote Registry service must be running on the machine where the ColdFusion server is running if ColdFusion is running on Windows 2000.

## **Configuring the Monitor**

For details on configuring the monitor, see “ColdFusion Server Monitor Settings” on page 445.



## ColdFusion Server Monitor Settings

<b>Description</b>	<p>Monitor the availability of a ColdFusion server (versions 4.5x) on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more ColdFusion server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “ColdFusion Server Monitor Overview” on page 443</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## ColdFusion Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the ColdFusion Server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>
<b>Counters</b>	<p>The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p><b>Note when working in template mode:</b> To update counters in template browsable monitors that need a target server, click the <b>Select measurement from</b> button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the <b>Server</b> field.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p>





# 20

---

## COM+ Server Monitor

This chapter includes the main concepts, tasks, and reference information for the COM+ Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ COM+ Server Monitor Overview on page 450

#### Tasks

- ▶ Configure the COM+ Monitoring Environment on page 451

#### Reference

- ▶ COM+ Server Monitor Settings on page 453

## **COM+ Server Monitor Overview**

Use the COM+ Server monitor to monitor the performance of COM+ software components registered and running on Microsoft Windows Server 2000 and Microsoft Windows Server 2003. When you specify the host and port number of this probe instance, SiteScope retrieves all the functions running on the COM+ server for your monitoring selection. Error and warning thresholds for the monitor can be set on one or more function measurements.

---

**Note:** The COM+ Server monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

---

This section also includes:

- ▶ “Setup Requirements” on page 450
- ▶ “Configuring the Monitor” on page 451

### **Setup Requirements**

The following are several key requirements for using the COM+ Server monitor:

- ▶ A COM+ probe component from HP must be installed and running on the target COM+ server you want to monitor. For details on how to perform this task, see “Configure the COM+ Monitoring Environment” on page 451.
- ▶ There must be HTTP connectivity between the SiteScope server and the server running the COM+ probe.
- ▶ To enable this monitor type in SiteScope, an Option license for the COM+ Server monitor must be obtained and input into SiteScope.

---

**Note:** You cannot have multiple SiteScope instances share one probe instance. You can have multiple COM+ Server monitors within a single SiteScope installation access the same probe instance (uniquely identified by the probe host and port). The probe cannot serve data to multiple SiteScope installations.

---

## Configuring the Monitor

For details on configuring the monitor, see “COM+ Server Monitor Settings” on page 453.

## Configure the COM+ Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Install the COM+ Probe” on page 451
- “Start the COM+ Probe” on page 452
- “Configure the Monitor Properties” on page 452

### 1 Install the COM+ Probe

A COM+ probe component must be installed and running on the target COM+ server you want to monitor.

- a** Go to the HP Software Support site (<http://www.hp.com/go/hpsupport>) and in the **Where do I find** section, click **Software patches**.

---

**Note:** To access the Patches search page, you must log in with your HP Passport user name and password.

---

- b** In the **Product** section, select **SiteScope**.
- c** In the optional search box, enter **COM+** and click **Search**.
- d** Download the COM+ probe from the results.
- e** After downloading, follow the instructions for installing the probe on the COM+ server to be monitored.

## **2 Start the COM+ Probe**

After successfully installing the probe, you must start it prior to running or defining a COM+ Server monitor, by invoking **mon\_cplus\_probe.exe** found in the COM+ probe's **bin** directory. By default, the installation creates this file at **C:\Program Files\Mercury Interactive\COMPlusMonitor\bin\**.

## **3 Configure the Monitor Properties**

Create a COM+ Server monitor, and specify the COM+ probe for the target COM+ server. The COM+ probe is queried for a list of available functions to monitor, and a browse tree is displayed. Select the COM+ functions or counters that you want to measure.

Complete the other COM+ Server monitor fields as required.

For details on the COM+ Server monitor settings, see “COM+ Server Monitor Settings” on page 453.

## COM+ Server Monitor Settings

<p><b>Description</b></p>	<p>The COM+ Server monitor monitors the performance of software components registered and running on Microsoft COM+ servers. When you specify the host and port number of this probe instance, SiteScope retrieves all the functions running on the COM+ server, for your monitoring selection. Error and warning thresholds for the monitor can be set on one or more function measurements.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “Configure the COM+ Monitoring Environment” on page 451</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “COM+ Server Monitor Overview” on page 450</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## COM+ Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>COM+ probe host name</b>	Enter the host name of the COM+ probe.
<b>COM+ probe port number</b>	Specify the port number of the COM+ probe. <b>Default value:</b> 8008
<b>Credentials</b>	<p>Select the option for providing the user name and password authorization to the COM+ probe.</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>HTTP proxy</b>	(Optional) A proxy server can be used to access the probe. Enter the domain name and port of an HTTP Proxy Server.
<b>Proxy server user name</b>	If the proxy server requires a name and password to access the probe, enter the name here. Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	If the proxy server requires a name and password to access the probe, enter the password here.

GUI Element	Description
<b>Timeout (seconds)</b>	<p>The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 60 seconds</p> <p><b>Note:</b> Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with a timeout value of more than 60 seconds to enable the server to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.</p>
<b>Counters</b>	<p>The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>





# 21

---

## Composite Monitor

This chapter includes the main concepts and reference information for the Composite monitor.

### **This chapter includes:**

#### Concepts

- ▶ Composite Monitor Overview on page 457

#### Reference

- ▶ Composite Monitor Settings on page 458

### **Composite Monitor Overview**

Each time the Composite monitor runs, it returns a status based on the number and percentage of items in the specified monitors and/or groups currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

Use this monitor is if you want to create complex monitor alert logic. For example, if you want to trigger an alert when:

- ▶ five or more monitors in a group of eight are in error
- ▶ three or more groups have monitors with errors in them
- ▶ you have two monitors, and exactly one is in error

then you could create a Composite monitor that went into error on these conditions, and then add alerts on the Composite monitor to take the desired actions.

If you need alert logic that is more complex than SiteScope's standard alerts allow, you can use the Composite monitor to create a customized alert behavior.



For details on configuring the monitor, see “Composite Monitor Settings” on page 458.

## Composite Monitor Settings


<p><b>Description</b></p>	<p>Designed to simplify the monitoring of complex network environments by checking the status readings of a set of other SiteScope monitors and/or monitor groups.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When using this monitor to monitor a URL monitor in which at least one of the steps uses a session cookie to send to the server instead of logging in each time, the Composite monitor saves the context including the cookie. This means that the login information does not need to be entered again, as the login credentials are sent in a cookie.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Composite Monitor Overview” on page 457</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Composite Monitor Settings






The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Items</b>	<p>Click the <b>Add</b>  button to open the Add Items dialog box, and select the monitors and/or groups that you want in the Composite monitor. For details on the Add Items dialog box, see “Add Items Dialog Box” on page 460.</p> <p>To remove items from the list, select the monitors and/or groups you want to remove (you can select multiple items using the CTRL or SHIFT keys), and click the <b>Delete</b>  button.</p>
<b>Run monitors</b>	<p>Select if you want the Composite monitor to control the scheduling of the selected monitors, as opposed to just checking their status readings.</p> <p>Monitors that are to be run this way should not also be run separately, so edit the individual monitors, set the <b>Frequency</b> box for that monitor to zero ("0"), and save the changes. Those monitors then run only when scheduled by the Composite monitor. This is useful if you want the monitors to run one after another or run at approximately the same time.</p> <p><b>Default value:</b> Not selected</p>
<b>Monitor delay (seconds)</b>	<p>If <b>Run monitors</b> is checked, this is the number of seconds to wait between running each monitor.</p> <p>This setting is useful if you need to wait for processing to occur on your systems before running the next monitor.</p> <p><b>Default value:</b> 0 seconds</p>
<b>Check all monitors in group(s)</b>	<p>When selected, all of the monitors in selected groups (and their subgroups) are checked and counted.</p> <p><b>Default value:</b> Not selected (each group is checked and counted as a single item when checking status readings).</p>

## Add Items Dialog Box

<b>Description</b>	<p>Enables you to select the monitors and/or groups that you want in the Composite monitor.</p> <p><b>To access:</b> In the monitor view, right-click a group and select <b>New &gt; Monitor</b>. Select the <b>Composite</b> monitor from the New Monitor Page, and click the <b>Add Items</b>  button.</p>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	► “Composite Monitor Overview” on page 457

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Add Selected Items</b>	Click to add the selected groups and/or monitors to the Composite monitor.
 SiteScope	Represents the SiteScope root directory.
	<p>Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors).</p> <p>If a group alert has been set up for the monitor group or subgroup, the alert  symbol is displayed next to the group icon.</p>
	<p>Represents a SiteScope monitor (enabled/disabled).</p> <p>If an alert has been set up for the monitor, the alert  symbol is displayed next to the monitor icon.</p>

# 22

---

## CPU Monitor

This chapter includes the main concepts and reference information for the CPU monitor.

### **This chapter includes:**

#### Concepts

- ▶ CPU Monitor Overview on page 461

#### Reference

- ▶ CPU Monitor Settings on page 463

### CPU Monitor Overview

Use the CPU monitor to monitor the percentage of CPU time that is currently being used on the server. By monitoring CPU usage, you can prevent poor system response times and outages before they occur.

Whether the servers in your infrastructure are running with a single CPU or with multiple CPUs, you only need to create one CPU monitor per remote server. If you have multiple CPUs, SiteScope reports on the average usage for all of them, as well as each individual CPU usage.

This section contains the following topics:

- ▶ “Status” on page 462
- ▶ “Scheduling the Monitor” on page 462
- ▶ “Troubleshooting and Limitations” on page 462
- ▶ “Configuring the Monitor” on page 463

## Status

The Status reading is the current value returned by this monitor; for example, 68% used. SiteScope displays an average for multiple CPU systems. On NT, this is the average CPU usage between runs of the monitor. On UNIX, this is the instantaneous CPU when the monitor runs.

The status is logged as either OK or warning. A warning status is returned if the CPU is in use more than 90% of the time.

## Scheduling the Monitor

In general, the CPU monitor does not need to be run as often as some of the other monitors. If you do not usually suffer from CPU problems, you can run it less frequently, perhaps every half hour or so. If you are prone to CPU usage problems, you should run it more frequently. All machines have short spikes of CPU usage, but the primary thing that you are looking for is high usage on a regular basis. This indicates that your system is overloaded and that you need to look for a cause.

## Troubleshooting and Limitations

**Problem:** Unable to monitor CPU usage on a clean installation of Linux RedHat 4.

**Cause:** The mpstat command that SiteScope runs on the monitored server as depicted in <SiteScope root directory>\Templates.os folder (/usr/bin/mpstat), is not deployed by default on a Linux machine. Linux installations come with a sysstat package.

**Solution:** In a terminal window, type `up2date sysstat` to deploy the mpstat package.

**Problem:** Getting invalid CPU value error message in <SiteScope root directory>\logs\RunMonitor.log file when using perfmon monitors on VMware host servers.

**Solution:** Use the VMWare Performance monitor to measure CPU on VMWare host servers.

## Configuring the Monitor

For details on configuring the monitor, see “CPU Monitor Settings” on page 463.

### CPU Monitor Settings

<b>Description</b>	<p>Reports the percentage of CPU time that is currently being used on the server.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>▶ The <b>Performance Counters Tool</b> is available when configuring this monitor to check performance counters on a specific machine in a Windows NT/2000 network (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Performance Counters Tool” on page 223.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “CPU Monitor Overview” on page 461</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## CPU Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the CPU you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed here. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>



GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>



# 23

---

## Database Counter Monitor

This chapter includes the main concepts and reference information for the Database Counter monitor.

### **This chapter includes:**

#### Concepts

- ▶ Database Counter Monitor Overview on page 467

#### Reference

- ▶ Database Counter Monitor Settings on page 471

### **Database Counter Monitor Overview**

Use the Database Counter monitor to make SQL queries for performance metrics from any JDBC-accessible database. This monitor provides optional support for calculating deltas and rates for metrics between monitor runs. You can monitor multiple counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning.

This monitor supports monitoring on any database with a valid JDBC driver that supports SQL queries.

This section also includes:

- ▶ “Setup Requirements and User Permissions” on page 468
- ▶ “Configuring the Monitor” on page 470

## Setup Requirements and User Permissions

The following are several key requirements for using the Database Counter monitor:

- ▶ You must have a copy of the applicable JDBC database driver file on the SiteScope server. Copy the downloaded driver file into the `<SiteScope root directory>\WEB-INF\lib` subdirectory. If the file is in zip format, do not unzip the file. Stop and restart the SiteScope service after copying the driver file to the SiteScope machine.
- ▶ You must know the syntax for accessing the database driver. Examples of common database driver strings are:
  - ▶ **sun.jdbc.odbc.JdbcOdbcDriver.** JDBC-ODBC Bridge Driver from Sun Microsystems.
  - ▶ **com.inet.tds.TdsDriver.** TDS driver from i-net Software for Microsoft SQL databases. This driver is deployed with SiteScope.
  - ▶ **com.inet.ora.OraDriver.** A driver from Oracle for Oracle databases. This driver is deployed with SiteScope.
  - ▶ **com.mercury.jdbc.sqlserver.SQLServerDriver.** DataDirect driver from DataDirect Technologies. It is an alternative to the TDS driver for those Microsoft SQL databases that use Windows NT authentication. This driver is deployed with SiteScope.
  - ▶ **oracle.jdbc.driver.OracleDriver.** JDBC thin driver for Oracle 7 and 8 databases. This driver is an Oracle product and is supplied by Oracle.
  - ▶ **com.mercury.jdbc.oracle.OracleDriver.** A driver for Oracle databases. This driver is deployed with SiteScope. When using the Oracle mercury driver, the database connection URL has the form of:  
`jdbc:mercury:oracle://<server name or IP address>:<database server port>;sid=<sid>`
  - ▶ **org.postgresql.Driver.** The database driver for the Postgresql database.
- ▶ You must know the syntax for the Database connection URL. The Database connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers.

Examples of common database connection URLs are:

- ▶ **jdbc:odbc:<dsname>**  
where <dsname> is the data source name in the system environment or configuration.
- ▶ **jdbc:inetdae:<hostname>:<port>**  
where <hostname> is the name of the host where the database is running and <port> is the port on which the database interfaces with the driver.
- ▶ **jdbc:mercury:sqlserver://<hostname>:1433;DatabaseName=master;AuthenticationMethod=type2**  
where <hostname> is the name of the host where the database is running.
- ▶ **jdbc:oracle:thin:@<hostname>:<port>:<dbname>**  
where <hostname> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <dbname> is the SID of the Oracle database instance.
- ▶ **jdbc:postgresql://<hostname>:<port>/<dbname>**  
where <hostname> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <dbname> is the name of the Postgresql database.
- ▶ Generally, you should only have one instance of each type of JDBC driver client installed on the SiteScope machine. If there is more than one instance installed, SiteScope may report an error and be unable to connect to the database. For example, installing two **classes12.zip** files from two different versions of Oracle is unlikely to work.

- ▶ You must have a database user login that SiteScope can use to access the database with **CREATE SESSION** system privileges. SiteScope is only able to run the SQL queries that this user has permission to run on the database.

---

**Note:** When Windows authentication is used to connect to the database, configure SiteScope using the following settings:

- ▶ **Database connection URL:** `jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>;AuthenticationMethod=type2.`
- ▶ **Database driver:** `com.mercury.jdbc.sqlserver.SQLServerDriver.`
- ▶ Leave the **Database User name** and **Database Password** boxes empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.

---

## Configuring the Monitor

For details on configuring the monitor, see “Database Counter Monitor Settings” on page 471.

## Database Counter Monitor Settings

<b>Description</b>	<p>The Database Counter monitor enables you to monitor the availability of any database through a JDBC driver. The error and warning thresholds for the monitor can be set on one or more database server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ The <b>Database Connection Tool</b> is available when configuring this monitor to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Database Connection Tool” on page 198.</li> </ul>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Database Counter Monitor Overview” on page 467</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Database Counter Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Database connection URL</b>	<p>Enter the connection URL to the database you want to connect to. The syntax is <code>jdbc:oracle:thin:@&lt;server name or IP address&gt;:&lt;database server port&gt;:&lt;sid&gt;</code>.</p> <p><b>Example:</b> To connect to the ORCL database on a machine using port 1521 use:  <code>jdbc:oracle:thin:@206.168.191.19:1521:ORCL</code>.            The colon (:) and the (@) symbols must be included as shown.</p> <p><b>Note for using Windows Authentication:</b> If you want to access the database using Windows authentication, enter <code>jdbc:mercury:sqlserver://&lt;server name or IP address&gt;:1433;DatabaseName=&lt;database name&gt;;AuthenticationMethod=type2</code> as the connection URL, and <code>com.mercury.jdbc.sqlserver.SQLServerDriver</code> as your database driver. Leave the <b>Database user name</b> and <b>Database password</b> boxes empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.</p>
<b>Query</b>	<p>Enter a SQL query that returns at least two columns of data. The values in the first column of data are interpreted as the labels for the entries in the each row. The values in the first row are treated as labels for each entry in the column.</p>
<b>Database driver</b>	<p>Enter the driver used to connect to the database.</p> <p><b>Example:</b> <code>org.postgresql.Driver</code></p>
<b>Database machine name</b>	<p>The identifier for the target database server, as it should be reported to HP Business Availability Center.</p>
<b>Divisor query</b>	<p>A SQL query that returns a single numeric value. The value of each counter is calculated by dividing the counter value as retrieved from the database divided by the Divisor Query value.</p>



GUI Element	Description
<b>No cumulative counters</b>	Select to turn off the default behavior of calculating the value of a counter as the difference between that counter's cumulative values (as retrieved from the database on consecutive monitor runs).
<b>No divide counters</b>	<p>Select to turn off the default behavior of calculating the value of a counter as the value retrieved from the database (or the delta of two values retrieved from the database over consecutive monitor runs) divided by some number.</p> <p>The divisor is either taken from the Divisor Query, or it is the elapsed time in seconds since the previous monitor run.</p>
<b>Credentials</b>	<p>Select the option for providing the user name and password to be used to access the database server.</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

## Database Connection Settings

<b>Description</b>	<p>The Database Connection Settings enable you to retrieve, share, and reuse database connections for database monitors that use any JDBC-compliant driver. When multiple database monitors use the same database, using a connection pool instead of an open connection for each monitor improves monitor performance and optimizes database server resource utilization.</p> <p>Connections can be shared regardless of monitor enter. For example, SiteScope database logger, database tools (Database Connection, Database Information), database alerts, and database monitors (Oracle Database, Database Counter, Database Query, DB2 8.x and 9.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>
<b>Important Information</b>	<p>You can set additional database options that affect all resources that connect to the database in the JDBC Global Options in the General Preferences container.</p>
<b>Useful Links</b>	<p>“JDBC Global Options” on page 1386</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Use connection pool</b>	<p>Enables SQL connection sharing. This means that you use a connection pool rather than open and close a new connection for each monitor query.</p> <p><b>Default value:</b> Selected</p>
<b>Physically close if idle connection count exceeds</b>	<p>This is the maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool.</p> <p><b>Default value:</b> 10</p>

GUI Element	Description
<b>Idle connection timeout</b>	The maximum amount of time, in seconds/minutes/hours/days, that a SQL connection remains unused after it has been returned to the SQL connection pool. When the time is exceeded, the connection is automatically closed. <b>Default value:</b> 5 minutes
<b>Query timeout</b>	The amount of time, in seconds/minutes/hours/days, to wait for execution of a SQL statement. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored. <b>Default value:</b> 1 minute



# 24

---

## Database Query Monitor

This chapter includes the main concepts, tasks, and reference information for the Database Query monitor.

### **This chapter includes:**

#### Concepts

- ▶ Database Query Monitor Overview on page 477

#### Tasks

- ▶ Configure the Database Query Monitoring Environment on page 483

#### Reference

- ▶ Database Query Monitor Settings on page 488

### **Database Query Monitor Overview**

Use the Database Query monitor to monitor the availability and proper functioning of your database application. If your database application is not working properly, the user may not be able to access Web content and forms that depend on the database. Most importantly, the user cannot complete e-commerce transactions that are supported by databases. You can also use the Database Query monitor to isolate performance bottlenecks. If the database interaction time and the associated user URL retrieval times are both increasing at about the same amount, the database is probably the bottleneck.

This monitor supports monitoring on any database with a valid JDBC driver that supports SQL queries.

This section contains the following topics:

- “What to Monitor” on page 478
- “Setup Requirements and User Permissions” on page 478
- “Troubleshooting and Limitations” on page 481
- “Configuring the Monitor” on page 482

## **What to Monitor**

Usually the most important thing to monitor in databases are the queries used by your most frequently used and most important Web applications. If more than one database is used, you must monitor each of the databases.

Each time the Database Query monitor runs, it returns a status, the time it takes to perform the query, the number of rows in the query result, and the first two fields in the first row of the result and writes them in the monitoring log file.

You can also monitor internal database statistics. The statistics provided by each database are different but may include items such as database free space, transaction log free space, transactions/second, and average transaction duration.

## **Setup Requirements and User Permissions**

The steps for setting up a Database Query monitor vary according to what database software you are trying to monitor. The following is an overview of the requirements for using the Database Query monitor:

- You must install or copy a compatible JDBC database driver or database access API into the required SiteScope directory location.

Many database driver packages are available as compressed (zipped) archive files or .jar files. Copy the downloaded driver file into the `<SiteScope root directory>\WEB-INF\lib` subdirectory. Do not unzip the file.

- ▶ You must know the syntax for accessing the database driver. Examples of common database driver strings are:
  - ▶ **sun.jdbc.odbc.JdbcOdbcDriver.** JDBC-ODBC Bridge Driver from Sun Microsystems.
  - ▶ **com.inet.tds.TdsDriver.** TDS driver from i-net Software for Microsoft SQL databases. This driver is deployed with SiteScope.
  - ▶ **com.inet.ora.OraDriver.** A driver from Oracle for Oracle databases. This driver is deployed with SiteScope.
  - ▶ **com.mercury.jdbc.sqlserver.SQLServerDriver.** Datadirect driver from DataDirect Technologies. It is an alternative to the TDS driver for those Microsoft SQL databases that use Windows NT authentication. This driver is deployed with SiteScope.
  - ▶ **oracle.jdbc.driver.OracleDriver.** JDBC thin driver for Oracle 7 and 8 databases. This driver is an Oracle product and is supplied by Oracle.
  - ▶ **com.mercury.jdbc.oracle.OracleDriver.** A driver for Oracle databases. This driver is deployed with SiteScope. When using the Oracle mercury driver, the database connection URL has the form of:  
`jdbc:mercury:oracle://<server name or IP address>:<database server port>;sid=<sid>`
- ▶ You must know the syntax for the database connection URL. The database connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers.

Examples of common database connection URLs are:

- ▶ **jdbc:odbc:<dsname>**  
 where <dsname> is the data source name in the system environment or configuration.
- ▶ **jdbc:inetdae:<hostname>:<port>**  
 where <hostname> is the name of the host where the database is running and <port> is the port on which the database interfaces with the driver.
- ▶ **jdbc:mercury:sqlserver://<hosthost>:1433;DatabaseName=master;AuthenticationMethod=type2**  
 where <hostname> is the name of the host where the database is running.

- ▶ **jdbc:oracle:thin:@<hostname>:<port>:<dbname>**  
where <hostname> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <dbname> is the name of the Oracle database instance.
- ▶ The database you want to monitor needs to be running, have a database name defined, and have at least one named table created in the database. In some cases, the database management software needs to be configured to enable connections by using the middleware or database driver.
- ▶ You need a valid user name and password to access and perform a query on the database. In some cases, the machine and user account that SiteScope is running on must be given permissions to access the database.
- ▶ You must know a valid SQL query string for the database instance and database tables in the database you want to monitor. Consult your database administrator to work out required queries to test.

---

**Note:** When Windows authentication is used to connect to the database, configure SiteScope using the following settings:

- ▶ **Database connection URL:** jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>;AuthenticationMethod=type2.
  - ▶ **Database driver:** com.mercury.jdbc.sqlserver.SQLServerDriver.
  - ▶ Leave the **Database user name** and **Database password** boxes empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.
-



## Troubleshooting and Limitations

This section contains the following troubleshooting and limitations for issues relating to working with the Database Query monitor:

### Possible Errors Using the Oracle Thin Driver

- **error, connect error, No suitable driver:** check for syntax errors in Database connection URL, such as dots instead of colons.
- **error, connect error, lo exception: The Network Adapter could not establish the connection:** in Database connection URL, check `jdbc:oracle:thin:@206.168.191.19:1521:ORCL`.
- **error, connect error, lo exception: Invalid connection string format, a valid format is: "host:port:sid":** in Database connection URL check `jdbc:oracle:thin:@206.168.191.19:1521:ORCL`.
- **error, connect error, Invalid Oracle URL specified: OracleDriver.connect:** in Database connection URL, check for a colon before the "@" `jdbc:oracle:thin:@206.168.191.19:1521:ORCL`.
- **Refused:OR=(CODE=12505)(EMFI=4)))):** in Database connection URL, check the database SID is probably incorrect (ORCL part). This error can also occur when the tcp address, or tcp port is incorrect. If this is the case, verify the tcp port and check with the your database administrator to verify the proper SID.
- **String Index out of range: -1:** in Database connection URL, check for the database server address, port, and the database SID.
- **error, driver connect error, oracle.jdbc.driver.OracleDriver:** check syntax in item Database driver.
- **error, driver connect error, oracle.jdbc.driver.OracleDriver:** check that driver is loaded in correct place.
- **error, connect error, No suitable driver:** check driver specified in item Database driver.
- **error, connect error, No suitable driver:** check for syntax errors in Database connection URL, such as dots instead of colons.

### **Possible Errors Using the MySQL Driver**

If, after setting this up, you get an authorization error in the Database Query monitor, then you may have to grant rights for the SiteScope machine to access the MySQL database. Consult the MySQL Database administrator for setting up privileges for the SiteScope machine to access the MySQL server.

### **Possible Errors with Sybase Database Monitoring**

- Verify you are using the correct driver for the version of Sybase you are monitoring. Enter `com.sybase.jdbc.SybDriver` for Sybase version 4.x. and `com.sybase.jdbc2.jdbc.SybDriver` for Sybase version 5.x.
- If you get the error: **error, driver connect error, com/sybase/jdbc/SybDriver**, verify that there are no spaces at the end of the driver name. Save the changes and try the monitor again.
- If you get the error: **connect error, JZ006: Caught IOException: java.net.UnknownHostException: dbservername**, verify the name of the database server in the **Database connection URL** box is correct.

### **Configuring the Monitor**

For task details, see “Configure the Database Query Monitoring Environment” on page 483.

For user interface details, see “Database Query Monitor Settings” on page 488.

## Configure the Database Query Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Access Oracle Databases Without Using ODBC - Optional” on page 483
- “Enable SiteScope to Monitor an Informix Database” on page 484
- “Enable SiteScope to Monitor a MySQL Database” on page 485
- “Enable SiteScope to Monitor a Sybase Database” on page 486
- “Configure the Monitor Properties” on page 487

### **1 Access Oracle Databases Without Using ODBC - Optional**

If you want to monitor an Oracle database without using ODBC, you can use the Oracle Thin JDBC Drivers.

- a** To set up SiteScope to use the JDBC Thin Drivers, download the Oracle Thin JDBC drivers from the Oracle Web site (may require service/support agreement with Oracle).
- b** Copy the downloaded driver package into the `<SiteScope root directory>\WEB-INF\lib` subdirectory.

---

**Note:** Do not extract the files from the archive file.

---

- c** Stop and restart the SiteScope service.

- d** Add a Database Query monitor within SiteScope, and configure the following settings in the Monitor Settings panel:

- ▶ **Database connection URL.** The format for the Oracle JDBC driver is:

```
jdbc:oracle:thin:@<tcp address>:<tcp port>:<database SID>
```

For example to connect to the ORCL database on a machine using port 1521 you would use:

```
jdbc:oracle:thin:@206.168.191.19:1521:ORCL
```

---

**Note:** After the word thin is a colon (:), and an at (@) symbol.

---

- ▶ **Database driver.** Enter the following string:  
oracle.jdbc.driver.OracleDriver.

For a list of possible errors using the Oracle Thin Driver, see “Possible Errors Using the Oracle Thin Driver” on page 481.

## 2 Enable SiteScope to Monitor an Informix Database

Monitoring a Informix database requires the use of a JDBC driver.

- a** Download the Informix JDBC driver from Informix. See the Informix Web site for details.
- b** Uncompress the distribution file.
- c** Open a DOS window and go to the **jdbc140jc2** directory.
- d** Unpack the driver by running the following command:  

```
c:\SiteScope\java\bin\java -cp . setup
```
- e** Copy **ifxjdbc.jar** to the **<SiteScope root directory>\WEB-INF\lib** subdirectory.
- f** Stop and restart SiteScope.

- g** Add a Database Query monitor within SiteScope, and configure the following settings in the Monitor Settings panel:
- ▶ **Database connection URL.** The format for the Informix JDBC driver is:
 

```
jdbc:informix-sqli://<database hostname>:<tcp port><database server>:INFORMIXSERVER=<database>
```
  - ▶ If you require a **Database user name** and **Database password**, the database connection URL format for the Informix JDBC driver is:
 

```
jdbc:informix-sqli://<database hostname>:<tcp port><database server>:INFORMIXSERVER=<database>;user=myuser;password=mypassword
```

For example, to connect to the Database Server sysmaster running on the machine called pond.thiscompany.com and the Database called maindbase, type:

```
jdbc:informix-sqli://pond.thiscompany.com:1526/sysmaster:INFORMIXSERVER=maindbase;
```
  - ▶ **Database driver.** Enter the Informix JDBC driver `com.informix.jdbc.IfxDriver`

### 3 Enable SiteScope to Monitor a MySQL Database

Monitoring a MySQL database requires the use of a JDBC driver.

- a** Download the MySQL JDBC driver from the MySQL web site (<http://www.mysql.com>).
- b** Uncompress the distribution file.
- c** Copy the .jar file into the `<SiteScope root directory>\WEB-INF\lib` directory.
- d** Stop and restart SiteScope.

- e Add a Database Query monitor within SiteScope, and configure the following settings in the Monitor Settings panel:
  - **Database connection URL.** The format for the MySQL JDBC driver is:  
`jdbc:mysql://<database hostname>[:<tcp port>]/<database>`  
For example to connect to the MySQL database "aBigDatabase" on a machine using the standard MySQL port number 3306 you would use:  
`jdbc:mysql://206.168.191.19/aBigDatabase`  
If you are using a different port to connect to the database, include that port number as part of the IP address.
  - **Database driver.** Enter the specification for the MySQL JDBC driver:  
`org.gjt.mm.mysql.Driver`

#### 4 Enable SiteScope to Monitor a Sybase Database

To use JDBC drivers with your Sybase SQL server, perform the following steps:

- a Obtain the driver for the version of Sybase that you are using. For example, for version 5.X databases you need **jconn2.jar**. If you have Jconnect, you should be able to find a driver in the Jconnect directory.
- b Place the zip file in the `<SiteScope root directory>\WEB-INF\lib` directory. Do not extract the zip file.
- c Stop and restart the SiteScope service.
- d Add a Database Query monitor within SiteScope, and configure the following settings in the Monitor Settings panel:
  - **Database connection URL.** Use the syntax of:  
`jdbc:sybase:Tds:hostname:port`  
For example to connect to SQL server named `bgsu97` listening on port 2408, you would enter:  
`jdbc:sybase:Tds:bgsu97:2408`
  - You can specify a database by using the syntax:  
`jdbc:sybase:Tds:hostname:port#/database`

For example to connect to SQL server named bgsu97 listening on port 2408 and to the database of quincy, you would enter:

```
jdbc:sybase:Tds:bgsu97:2408/quincy
```

- ▶ **Database driver.** Enter `com.sybase.jdbc.SybDriver` (for Sybase version 4.x) or `com.sybase.jdbc2.jdbc.SybDriver` (for Sybase version 5.x).
- ▶ Enter the **Database user name** and **Database password**.
- ▶ Enter a query string for a database instance and table in the Sybase database you want to monitor.

For example, `Sp_help` should work and return something similar to:  
good, 0.06 sec, 27 rows, KIRK1, dbo, user table

Alternately, the query string `select * from spt_ijdbc_mda` should return something similar to:

```
Monitor: good, 0.06 sec, 175 rows, CLASSFORNAME, 1, create table
#tmp_class_for_name (xtbinaryoffrow image null),
sp_ijdbc_class_for_name(?), select * from #tmp_class_for_name, 1, 7,
12000, -1
```

## 5 Configure the Monitor Properties

Complete the Database Query monitor configuration. For details on the monitor settings, see “Database Query Monitor Settings” on page 488.

---

**Note:** You may want to monitor your most critical and most common queries frequently, every 2-5 minutes. Database statistics that change less frequently can be monitored every 30 or 60 minute.

---



## Database Query Monitor Settings

<p><b>Description</b></p>	<p>Checks that a database is working correctly by connecting to it and performing a query. Optionally, it can check the results of a database query for expected content.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>Database Connection Tool</b> is available when configuring this monitor to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Database Connection Tool” on page 198.</li> </ul>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “Configure the Database Query Monitoring Environment” on page 483</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Database Query Monitor Overview” on page 477</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>



## Database Query Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Database connection URL</b>	<p>Enter a URL to a database connection (no spaces are allowed in the URL). One way to create a database connection is to use ODBC to create a named connection to a database.</p> <p><b>Example:</b> First use the ODBC control panel to create a connection called <code>test</code>. Then, enter <code>jdbc:odbc:test</code> as the connection URL.</p> <p><b>Note for using Windows Authentication:</b> If you want to access the database using Windows authentication, enter <code>jdbc:mercury:sqlserver://&lt;server name or IP address&gt;:1433;DatabaseName=&lt;database name&gt;;AuthenticationMethod=type2</code> as the connection URL, and <code>com.mercury.jdbc.sqlserver.SQLServerDriver</code> as your database driver. Leave the <b>Database user name</b> and <b>Database password</b> boxes empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.</p>
<b>Database driver</b>	<p>Enter the java class name of the JDBC database driver.</p> <p>The default driver uses ODBC to make database connections. SiteScope uses the same database driver for both primary and backup database connections.</p> <p>If a custom driver is used, the driver must also be installed in the <code>&lt;SiteScope root directory&gt;\WEB-INF\lib</code> directory.</p> <p><b>Default value:</b> <code>sun.jdbc.odbc.JdbcOdbcDriver</code></p>

GUI Element	Description
<p><b>Database user name</b></p>	<p>Enter the user name used to log in to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystems JDBC-ODBC bridge driver, sun.jdbc.odbc.JdbcOdbcDriver), you can leave this blank and choose NT Authentication when you setup the ODBC connection.</p> <p>With NT Authentication, SiteScope connects using the login account of the SiteScope service.</p> <p><b>Note:</b> The specified user name must have privileges to run the query specified for the monitor.</p>
<p><b>Database password</b></p>	<p>Enter a password used to login to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystems JDBC ODBC bridge driver (sun.jdbc.odbc.JdbcOdbcDriver), you can leave this blank and choose NT Authentication when you create the ODBC connection.</p> <p>With NT Authentication, SiteScope connects using the login account of the SiteScope service.</p>
<p><b>Query</b></p>	<p>Enter the SQL query to test.</p> <p><b>Example:</b> select * from sysobjects</p>

GUI Element	Description
<b>Match content</b>	<p>Enter a string of text to check for in the query result. If the text is not contained in the result, the monitor displays no match on content. This works for XML tags as well.</p> <p>You may also perform a Perl regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p><b>Example:</b> <code>/href=Doc\d+\.html/</code> or <code>/href=doc\d+\.html/i</code></p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression.</p> <p><b>Example:</b> <code>/Temperature: (d+)/</code> would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ The search is case sensitive.</li> <li>➤ You can click the <b>Open Tool</b> button to use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</li> </ul>
<b>File path</b>	<p>Enter the name of the file that contains the query you want to run. The file should be in a simple text format.</p> <p>Use this function as an alternative to the Query text box for complex queries or queries that change and are updated by an external application.</p>

GUI Element	Description
<b>Column labels</b>	<p>Enter the field labels for the two columns returned by the query, separated by a comma (","). These column labels are used as data labels in SiteScope reports for Database Query Monitors.</p> <p><b>Note:</b> The field labels should be two of the labels that are returned by the Query string entered above.</p>
<b>Database machine name</b>	<p>If you are reporting monitor data to an installation of HP Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in an HP Business Availability Center report.</p>

### Database Connection Settings

<b>Description</b>	<p>The Database Connection Settings enable you to retrieve, share, and reuse database connections for database monitors that use any JDBC-compliant driver. When multiple database monitors use the same database, using a connection pool instead of an open connection for each monitor improves monitor performance and optimizes database server resource utilization.</p> <p>Connections can be shared regardless of monitor type. For example, SiteScope database logger, database tools (Database Connection, Database Information), database alerts, and database monitors (Oracle Database, Database Counter, Database Query, DB2 8.x and 9.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>
<b>Important Information</b>	<p>You can set additional database options that affect all resources that connect to the database in the JDBC Global Options in <b>Preferences &gt; General Preferences</b>.</p>
<b>Useful Links</b>	<p>"JDBC Global Options" on page 1386</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Use connection pool</b>	<p>Enables SQL connection sharing. This means that you use a connection pool rather than open and close a new connection for each monitor query.</p> <p><b>Default value:</b> Selected</p>
<b>Physically close if idle connection count exceeds</b>	<p>The maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool.</p> <p><b>Default value:</b> 10</p>
<b>Idle connection timeout</b>	<p>The maximum amount of time, in seconds/minutes/hours/days, that a SQL connection remains unused after it has been returned to the SQL connection pool. When the time is exceeded, the connection is automatically closed.</p> <p><b>Default value:</b> 5 minutes</p>
<b>Query timeout</b>	<p>The amount of time, in seconds/minutes/hours/days, to wait for execution of a SQL statement. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored.</p> <p><b>Default value:</b> 1 minute</p>



# 25

---

## DB2 8.x and 9.x Monitor

This chapter includes the main concepts and reference information for the DB2 8.x and 9.x monitor.

### **This chapter includes:**

#### Concepts

- ▶ DB2 8.x and 9.x Monitor Overview on page 495

#### Reference

- ▶ DB2 8.x and 9.x Monitor Settings on page 497

### **DB2 8.x and 9.x Monitor Overview**

Use the DB2 8.x and 9.x monitor to monitor DB2 8.x and 9.x servers for availability and proper functioning. You can monitor multiple parameters or counters with a single monitor instance. This enables you to monitor server loading for performance, availability, and capacity planning. Create a separate DB2 monitor instance for each Database in your IBM DB2 environment.

This section contains the following topics:

- ▶ “Setup Requirements” on page 496
- ▶ “DB2 8.x and 9.x Topology Settings” on page 496
- ▶ “Configuring the Monitor” on page 497

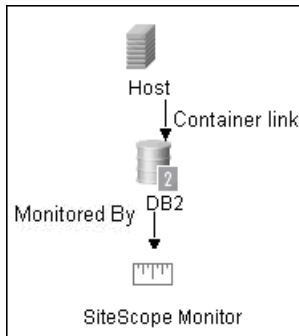
## Setup Requirements

The following are several key requirements for using the DB2 8.x and 9.x monitor:

- ▶ JDBC drivers for connecting to the DB2 Database server. These can be found in your DB2 server installation directories. Copy the **db2jcc.jar** file to the **<SiteScope root directory>\java\lib\ext** folder.
- ▶ This monitor uses the Snapshot mirroring functionality supported by DB2. You must enable the Snapshot Mirror on your DB2 instance to retrieve counters. See the information from the IBM DB2 documentation (<http://www-128.ibm.com/developerworks/db2/library/techarticle/dm-0408hubel/>).

## DB2 8.x and 9.x Topology Settings

The DB2 8.x and 9.x monitor can identify the topology of the DB2 system being monitored. If **Include topology data when reporting to HP Business Availability Center** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160 in the HP Business Availability Center Documentation Library.



## Configuring the Monitor

For details on configuring the monitor, see “DB2 8.x and 9.x Monitor Settings” on page 497.

### DB2 8.x and 9.x Monitor Settings

<p><b>Description</b></p>	<p>Monitors the availability and performance statistics of an IBM DB2 8.x or 9.x database. The error and warning thresholds for the monitor can be set on up to ten DB2 server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ The <b>Database Connection Tool</b> is available when configuring this monitor to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Database Connection Tool” on page 198.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “DB2 8.x and 9.x Monitor Overview” on page 495</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## DB2 8.x and 9.x Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>DB2 server</b>	Enter the address or name of the server where the DB2 database is running.
<b>Port</b>	The port on which the DB2 database accepts connections. <b>Default value:</b> 50000
<b>Database</b>	Enter the DB2 database node name that you want to monitor. <b>Default value:</b> sample <b>Example:</b> DB2 is the default node name created by DB2 installation.
<b>Credentials</b>	Select the option for providing the user name and password to be used to access the DB2 database server. <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (selected by default). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>Partition</b>	Partition to monitor. -1 is the current partition; -2 is all partitions. <b>Default value:</b> -1

GUI Element	Description
<b>Calculate rate</b>	<p>Select to calculate rates for counter values rather than the actual values returned from the monitored server.</p> <p><b>Example:</b> If a counter counts logins and every second an average of two users log in to the database, the counter keeps growing. Selecting this option, the monitor displays the value 2, which means 2 user logins per second.</p>
<b>Counters</b>	<p>The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

## Database Connection Settings

<b>Description</b>	<p>The Database Connection Settings enable you to retrieve, share, and reuse database connections for database monitors that use any JDBC-compliant driver. When multiple database monitors use the same database, using a connection pool instead of an open connection for each monitor improves monitor performance and optimizes database server resource utilization.</p> <p>Connections can be shared regardless of monitor type. For example, SiteScope database logger, database tools (Database Connection, Database Information), database alerts, and database monitors (Oracle database, Database Counter, Database Query, DB2 8.x and 9.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>
<b>Important Information</b>	<p>You can set additional database options that affect all resources that connect to the database in the JDBC Global Options in the General Preferences container.</p>
<b>Useful Links</b>	<p>“JDBC Global Options” on page 1386</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Use connection pool</b>	<p>If this check box is selected, SQL connection sharing is enabled. This means that you use a connection pool rather than open and close a new connection for each monitor query.</p> <p><b>Default value:</b> Selected</p>
<b>Physically close if idle connection count exceeds</b>	<p>The maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool.</p> <p><b>Default value:</b> 10</p>

GUI Element	Description
<b>Idle connection timeout</b>	The maximum amount of time, in seconds/minutes/hours/days, that a SQL connection remains unused after it has been returned to the SQL connection pool. When the time is exceeded, the connection is automatically closed. <b>Default value:</b> 5 minutes
<b>Query timeout</b>	The amount of time, in seconds/minutes/hours/days, to wait for execution of a SQL statement. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored. <b>Default value:</b> 1 minute



# 26

---

## Directory Monitor

This chapter includes the main concepts and reference information for the Directory monitor.

### **This chapter includes:**

#### Concepts

- ▶ Directory Monitor Overview on page 503

#### Reference

- ▶ Directory Monitor Settings on page 504

### **Directory Monitor Overview**

Use the Directory monitor to monitor directories that contain log files or other files that tend to grow and multiply unpredictably. You can instruct SiteScope to notify you if either the number of files or total disk space used gets out of hand. You can also use this to monitor directories in which new files are added and deleted frequently. For example, in the case of an FTP directory, you probably want to watch both the number of files in the directory and the files contained in the directory. The Directory monitor supports monitoring remote servers running on HP NonStop operating systems.

You can set up thresholds for this monitor based on the time in minutes since the latest time a file in the directory has been modified, as well as the time in minutes since the first time a file in the directory has been modified.

Because the uses for the Directory monitor vary so greatly, there is no one interval that works best. Keep in mind that if you are watching a directory that contains a lot of files and sub directories, this monitor may take longer to run.

For details on configuring the monitor, see “Directory Monitor Settings” on page 504.

## Directory Monitor Settings

<p><b>Description</b></p>	<p>The Directory monitor watches an entire directory and reports on the total number of files in the directory, the total amount of disk space used, and the time (in minutes) since any file in the directory was modified. This information is useful if you have limited disk space, you want to monitor the number of files written to a specific directory, or you want to know the activity level in a certain directory.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor supports monitoring remote servers running on HP NonStop operating systems.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Directory Monitor Overview” on page 503</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>



## Directory Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the directory you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> Monitoring log files using SSH on Windows platforms is supported for this monitor only if the remote SSH server supports SSH File Transfer Protocol.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>

GUI Element	Description
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>
<b>Directory path</b>	<p>Enter the directory that you want to monitor.</p> <ul style="list-style-type: none"> <li>▶ To monitor directories on a remote Windows NT/2000 server through NetBIOS, the path should contain the name of the shared folder for remote NetBIOS servers. You can also specify an absolute path of the directory on the remote machine without specifying the server name. For example, if you type <code>c:\test</code>, the remote directory is accessed as <code>\\Server\C\$\test</code>.</li> <li>▶ To monitor a directory on a remote Windows SSH machine, the path must be relative to the home directory of the user account used to log in to the remote machine.</li> <li>▶ To monitor a directory on remote UNIX machines, the path must be relative to the home directory of the UNIX user account used to log in to the remote machine. You must also select the corresponding remote UNIX server in the <b>Servers</b> box described above. For details on which UNIX user account to use for the applicable remote server, see “Remote Servers Overview” on page 1276.</li> </ul> <p>To monitor a directory that is created automatically by some application and the directory path includes date or time information, you can use SiteScope's special data and time substitution variables in the path of the directory. For details, see “SiteScope Date Variables” on page 274.</p>

GUI Element	Description
<b>No subdirectories</b>	Select this box if you do not want SiteScope to count subdirectories.
<b>File name match</b>	Enter text or an expression to match against (optional). Only file names which match are counted in the totals.



# 27

---

## Disk Space Monitor

This chapter includes the main concepts and reference information for the Disk Space monitor.

### **This chapter includes:**

#### Concepts

- ▶ Disk Space Monitor Overview on page 509

#### Reference

- ▶ Disk Space Monitor Settings on page 511

### **Disk Space Monitor Overview**

Use the Disk Space monitor to monitor the amount of disk space that is currently in use on your server. Having SiteScope verify that your disk space is within acceptable limits can save you from a crashed system and corrupted files.

The disk space monitor does not require many resources, so you can check it as often as every 15 seconds, but every 10 minutes should be sufficient. You may want to have SiteScope run a script (using a Script Alert) that deletes all files in certain directories, such as `/tmp`, when disk space becomes constrained. For details on using a Script Alert, see “Working with Script Alerts” on page 1977.

The Disk Space monitor supports monitoring remote servers running on HP NonStop operating systems.

This section contains the following topics:

- “Setup Requirements and User Permissions” on page 510
- “Troubleshooting and Limitations” on page 510
- “Configuring the Monitor” on page 510

### **Setup Requirements and User Permissions**

You must have domain privileges or authenticated access to the remote Windows or UNIX server, and specify valid user credentials. The user specified in the **Credentials** section must have sufficient permissions to connect to and gather information from the remote server disk drives. On UNIX systems, the defined user must have privileges to execute a command to retrieve available mounted disks (for example, on Linux: `/bin/df -k <disk>`).

### **Troubleshooting and Limitations**

Disk performance counters are unavailable by default in standard Windows 2000 installations. To monitor disk drives on servers running Windows 2000, you must enable these disk counters. Use the `diskperf -y` command line on each Windows 2000 machine you want to monitor disk space, and then reboot each server. You should then be able to select the disk drives for those servers in the Disk Space monitor dialog box.

### **Configuring the Monitor**

For details on configuring the monitor, see “Disk Space Monitor Settings” on page 511.

 **Disk Space Monitor Settings**

<b>Description</b>	<p>The Disk Space monitor tracks how much disk space is currently in use on your server.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This monitor supports:             <ul style="list-style-type: none"> <li>▶ WMI (Windows Management Instrumentation) as a method for gathering statistics.</li> <li>▶ Monitoring remote servers running on HP NonStop operating systems.</li> </ul> </li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>▶ The <b>Performance Counters Tool</b> is available when configuring this monitor to check performance counters on a specific machine in a Windows NT/2000 network (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Performance Counters Tool” on page 223.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Disk Space Monitor Overview” on page 509</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Disk Space Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<p><b>Server</b></p>	<p>The server where the disk space you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<p><b>Browse Servers</b></p>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>



GUI Element	Description
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>
<b>Disk/File system</b>	Select the disk drive that you want to monitor from the list.



# 28

---

## DHCP Monitor

This chapter includes the main concepts, tasks, and reference information for the DHCP monitor.

### **This chapter includes:**

#### Concepts

- ▶ DHCP Monitor Overview on page 515

#### Tasks

- ▶ Configure the DHCP Monitoring Environment on page 516

#### Reference

- ▶ DHCP Monitor Settings on page 517

### **DHCP Monitor Overview**

Use the DHCP monitor to monitor your DHCP servers to verify that they are working properly. If your DHCP server fails, machines relying on DHCP are unable to acquire a network configuration when rebooting. Additionally, as DHCP address leases expire on already-configured machines, those machines drop off the network when the DHCP server fails to renew their address lease.

Most networks have a DHCP server listening for DHCP requests. This monitor finds DHCP servers by broadcasting a request for an IP address and waiting for a DHCP server to respond.

Each time the DHCP monitor runs, it returns a status and writes it in the monitoring log file. It also writes the total time it takes to receive and release an IP address in the log file. Your DHCP server is a critical part of providing functionality to other hosts on your network, so it should be monitored about every 10 minutes.

The SiteScope DHCP monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running. The DHCP monitor type does not appear in the interface until this library is installed. For details on how to perform this task, see “Install the jDHCP Library” on page 516.

For details on the monitor user interface, see “DHCP Monitor Settings” on page 517.

## Configure the DHCP Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Install the jDHCP Library” on page 516
- “Configure the Monitor Properties” on page 516

### 1 Install the jDHCP Library

Install the Java DHCP library on the server where SiteScope is running.

- a** Download the jDHCP library (either in .zip or in .tar.gz format) from <http://www.dhcp.org/javadhcp/>.
- b** Extract the file named **JDHCP.jar** and copy it to the **<SiteScope root directory>\WEB-INF\lib** directory.
- c** After installing the **JDHCP.jar** file, restart the SiteScope service.

### 2 Configure the Monitor Properties

Complete the DHCP monitor configuration. For details on the monitor settings, see “DHCP Monitor Settings” on page 517.

## DHCP Monitor Settings

<b>Description</b>	<p>Checks a DHCP Server by using the network. It verifies that the DHCP server is listening for requests and that it can allocate an IP address in response to a request.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running. The DHCP monitor type does not appear in the interface until this library is installed. For more information, see “Install the jDHCP Library” on page 516.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the DHCP Monitoring Environment” on page 516</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “DHCP Monitor Overview” on page 515</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## DHCP Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Timeout	Enter the time, in seconds, to wait for an IP address. <b>Default value:</b> 10 seconds
Requested client address	Optionally, the IP address to request from the DHCP server.

# 29

---

## DNS Monitor

This chapter includes the main concepts and reference information for the DNS monitor.

### **This chapter includes:**

#### Concepts

- ▶ DNS Monitor Overview on page 519

#### Reference

- ▶ DNS Monitor Settings on page 522

### **DNS Monitor Overview**

Use the DNS monitor to monitor your DNS servers to verify that they are working properly. If your DNS server is not working properly, you cannot get out on the network, and people trying to reach your server are not able to find it using the server name (they can connect to it using the IP address only).

Most companies have both a primary and a secondary DNS server. If your company employs a firewall, these DNS servers may sit outside the firewall with another DNS server located inside the firewall. This internal DNS server provides domain name service for internal machines. It is important to monitor all of these servers to check that each is functioning properly.

If you have both a primary and secondary DNS server outside your firewall and an internal DNS server inside your firewall, you should monitor your internal server and your primary DNS server every 2-5 minutes. You can monitor the secondary DNS server less frequently (about every 10-15 minutes). To use this monitor, the TCP/IP protocol must be installed.

This section also includes:

- ▶ “Troubleshooting and Limitations” on page 520
- ▶ “Configuring the Monitor” on page 521

### **Troubleshooting and Limitations**

The following are guidelines for troubleshooting DNS monitor problems:

- ▶ If the SiteScope server cannot reach a DNS server that is running (no ping to host), and there are no network connectivity issues, check the TCP/IP client configuration settings on the DNS server. Also verify that the DNS server itself does not a connectivity issue.
- ▶ If the SiteScope server does not get a response to name resolution requests (even though it can ping the DNS server), ask your network administrator to verify that the DNS Server service is enabled and running on the DNS server.
- ▶ If the DNS server responds to queries for name resolution but with the incorrect information, it might be because the DNS server has incorrect or outdated information in its resource records for the specific zone. This situation can be due to a number of issues, including the following (should be managed by network administrator):
  - ▶ If administrators are manually creating and updating resource records, the incorrect information might have been inserted into the zone database file by the individual updating the resource records. To rectify this issue, you would have to manually verify the validity of each resource record.
  - ▶ If the DNS server is configured for dynamic updates, verify that dynamic updates have indeed occurred. If no dynamic updates have occurred, this would be the reason that the DNS server responded to SiteScope requests with outdated information. If the issue still persists, verify that the DNS server is configured for dynamic updates.



- The DNS server might be incorrectly resolving names from a secondary DNS server due to zone transfer not occurring for the specific secondary DNS server. This would result in the secondary zone database file containing the incorrect information. To rectify this issue, manually force a zone transfer to ensure that the secondary DNS zone database file contains updated information.

### **Configuring the Monitor**

For details on configuring the monitor, see “DNS Monitor Settings” on page 522.



## DNS Monitor Settings

<p><b>Description</b></p>	<p>The DNS monitor:</p> <ul style="list-style-type: none"> <li>▶ check a Domain Name Server by using the network</li> <li>▶ verifies that the DNS server is accepting requests</li> <li>▶ verifies that the address for a specific domain name can be found</li> <li>▶ returns a status and writes it in the monitoring log file with each running</li> </ul> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>DNS Lookup Tool</b> is available when configuring this monitor to look up names from a Domain Name Server and show you the IP address for a domain name (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “DNS Lookup Tool” on page 203.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “DNS Monitor Overview” on page 519</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## DNS Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>DNS server address</b>	Enter the IP address of the DNS server that you want to monitor. <b>Example:</b> 206.168.191.1
<b>Host to resolve</b>	Enter the host name to lookup. If you only want to verify that your DNS server is operating, the host name you enter here can be any valid host name or domain name. <b>Example:</b> demo.thiscompany.com To verify that a domain name resolves to a specific IP address, enter the IP address that corresponds to the host name you enter in the <b>Expected IP address</b> box.
<b>Expected IP address</b>	(Optional) You can use the DNS monitor to verify that a host name or domain name resolves to the correct IP address or addresses. Enter the IP address or addresses that are mapped to the <b>Host to resolve</b> (domain name) entered above. <b>Note:</b> If you enter more than one IP address, the monitor reports a status of good, even if only one of the IP addresses that you enter is mapped correctly to the <b>Host to resolve</b> . When using this option, the monitor only reports an error if none of the IP addresses entered here are mapped to the given <b>Host to resolve</b> . When entering multiple IP addresses, separate them with a comma (",").



# 30

---

## e-Business Transaction Monitor

This chapter includes the main concepts, tasks, and reference information for the e-Business Transaction monitor.

### **This chapter includes:**

#### Concepts

- ▶ e-Business Transaction Monitor Overview on page 525

#### Tasks

- ▶ Configure the e-Business Transaction Monitoring Environment on page 528

#### Reference

- ▶ e-Business Transaction Monitor Settings on page 530

### e-Business Transaction Monitor Overview

Use this monitor to verify that an end-to-end transaction and associated processes complete properly. For example, you could use this monitor to verify that the following steps, each of which is a step in a single transaction, run properly:

- ▶ Place an order on a Web site (see “Working with the URL Sequence Monitor” on page 985)
- ▶ Check that the order status was updated (see “Working with the URL Sequence Monitor” on page 985)
- ▶ Check that a confirmation email was received (see “Mail Monitor Overview” on page 607)

- ▶ Check that the order was added to the order database (see “Database Query Monitor Overview” on page 477)
- ▶ Check that the order was transferred to a legacy system (see “Script Monitor Settings” on page 840)

You should monitor any multi-step transaction process that causes other updates or actions in your systems. Monitor each of the actions taken to check that updates were performed properly and that actions were carried out successfully.

Using this example, you would first create the URL Sequence monitor, Mail monitor, Database monitor, and applicable Script monitor needed to verify each step of the chain. Then you would create an e-Business Transaction monitor and select each of these SiteScope monitors as a group in the order they should be run. If any one monitor indicates a failure, the e-Business Transaction monitor reports an error.

Each time the e-Business Transaction monitor runs, it returns a status based on the number and percentage of items in the specified monitors and/or groups currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

This section contains the following topics:

- ▶ “Editing the Order of the Monitors in the Chain” on page 527
- ▶ “Setting up Monitors for the e-Business Chain” on page 527
- ▶ “Configuring the Monitor” on page 527

## Editing the Order of the Monitors in the Chain

By default, the Add e-Business Transaction monitor page lists monitor groups and individual monitors in alphabetical order. To have the e-Business Transaction monitor run the chain of monitors in the proper order, they must appear in the proper order in the **Selected** table on the New e-Business Transaction Monitor page. You can do this by selecting the individual monitors in the order in which they should be run.

---

**Note:** To control the order of the monitors in the chain, you should select monitors and not groups. If you select groups to run in the e-Business Transaction monitor, they are run at random and not by group order.

---

## Setting up Monitors for the e-Business Chain

Before you can add an e-Business Transaction monitor, you must define other SiteScope monitors that report on the actions and results of the steps in the sequence chain. Using the example from the usage guidelines above, you can create one or more URL Sequence monitor for verifying the sequence of online actions, a Mail monitor to confirm that an email acknowledgement is sent, and a Database Query monitor to see that information entered online is logged into a database.

For details on setting up a URL sequence chain monitor, see “Configure the e-Business Transaction Monitoring Environment” on page 528.

## Configuring the Monitor

For task details, see “Configure the e-Business Transaction Monitoring Environment” on page 528.

For user interface details, see “e-Business Transaction Monitor Settings” on page 530.

## **Configure the e-Business Transaction Monitoring Environment**

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- ▶ “Set Up Monitors for the e-Business Chain” on page 528
- ▶ “Add and Configure the e-Business Transaction Monitor” on page 529

### **1 Set Up Monitors for the e-Business Chain**

Before you can add an e-Business Transaction monitor, you must define other SiteScope monitors that report on the actions and results of the steps in the sequence chain.

- a** Create a new group that contains all the individual monitors to be included in the sequence chain.
- b** Open the new monitor group, and add the first individual monitor type needed for the sequence (for example, “URL Sequence Monitor” on page 983).

---

**Note:** Monitors should be added in the order that they are run in the chain. For example, select a URL Sequence monitor which triggers an email event before you select the Mail monitor to check for the email.

To control the order of the monitors in the chain, you should select monitors and not groups. If you select groups to run in the e-Business Transaction monitor, they are run at random and not by group order.

---

- c** If necessary, set up the values to be passed from one monitor to another in the chain.



- d** Add the other monitors for this transaction chain in the required order of execution into the group.

---

**Note:** The individual monitors run by the e-Business Transaction monitor should generally not be run separately by SiteScope. You should make sure that the **Frequency** setting for each of these monitors is set to zero ("0").

---

- e** Create a new group or open an existing group that contains the e-business transaction chain monitor you are creating.
- f** Click **New > Monitor** and select the **e-Business Transaction** monitor.

## **2 Add and Configure the e-Business Transaction Monitor**

Complete the e-Business Transaction monitor configuration. For details on configuring the monitor settings, see “e-Business Transaction Monitor Settings” on page 530.

 **e-Business Transaction Monitor Settings**

<b>Description</b>	<p>Verifies that the multiple tasks that make up an online transaction are completed properly. This includes:</p> <ul style="list-style-type: none"> <li>▶ Successful navigation through a series of URLs</li> <li>▶ Transmission of an email confirming the sequence.</li> <li>▶ Logging the information into a database file.</li> </ul> <p>Runs a sequence of other SiteScope monitors, checking that each monitor returns a status of OK. Reports an Error status if any monitor in the sequence fails.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the e-Business Transaction Monitoring Environment” on page 528</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “e-Business Transaction Monitor Overview” on page 525</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## e-Business Transaction Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>Monitor delay (seconds)</b>	<p>Enter a number of seconds to wait between running each monitor.</p> <p>This setting is useful if you need to wait for processing to occur on your systems before running the next monitor.</p> <p><b>Default value:</b> 0 seconds</p>
<b>When error</b>	<p>Choose how you want errors during the sequence to be handled:</p> <ul style="list-style-type: none"> <li>▶ <b>Continue to run the remainder of the monitors.</b> This runs every monitor no matter what the status of a given monitor is.</li> <li>▶ <b>Stop and do not run any of the remaining monitors.</b> This stops running the list of monitors immediately, if a monitor returns an error.</li> <li>▶ <b>Run the last monitor.</b> This runs the last monitor in the list. It is useful if a monitor is used for closing or logging off a session opened in a previous monitor.</li> </ul>
<b>Single session</b>	<p>Select this box if you want any URL monitors to use the same network connection and the same set of cookies.</p> <p>This is useful if you are using the e-Business Transaction monitor to group several URL Sequence monitors and do not want to include the login steps as part of each transaction.</p>

GUI Element	Description
<b>Item Settings</b>	
<b>Items</b>	<p>Using the control key or equivalent, double-click the set of monitors that make up the e-Business Transaction monitor to move them to the <b>Selected</b> column.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ Monitors are run in the order that they are listed in their group. For details, see “Editing the Order of the Monitors in the Chain” on page 527.</li> <li>▶ To control the order of the monitors in the chain, select monitors and not groups. If you select groups, they are run at random and not by group order.</li> </ul>

# 31

---

## F5 Big-IP Monitor

This chapter includes the main concepts and reference information for the F5 Big IP monitor.

### **This chapter includes:**

#### Concepts

- ▶ F5 Big-IP Monitor Overview on page 533

#### Reference

- ▶ F5 Big-IP Monitor Settings on page 534

### **F5 Big-IP Monitor Overview**

Use the F5 Big-IP monitor to monitor the content of event logs and other data from F5 Big-IP 4.0 load balancing device. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate F5 Big-IP monitor instance for each F5 Big-IP load balancing device in your environment.

For details on configuring the monitor, see “F5 Big-IP Monitor Settings” on page 534.

## F5 Big-IP Monitor Settings

<b>Description</b>	<p>Allows you to monitor the statistics of a F5 Big-IP load balancing device using SNMP. The error and warning thresholds for the monitor can be set on one or more load balancer statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ The <b>SNMP Browser Tool</b> is available when configuring this monitor to verify the connection properties of an SNMP agent and to gain more information about the MIBs which that agent implements (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “SNMP Browser Tool” on page 237.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “F5 Big-IP Monitor Overview” on page 533</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## F5 Big-IP Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>SNMP Connection Settings</b>	
<b>Server</b>	Enter the name of the server you want to monitor.
<b>SNMP version</b>	Select the version of SNMP to use when connecting. Supports SNMP version 1, 2, and 3. Selecting V3 enables you to enter V3 settings in the SNMP V3 settings panel. <b>Default value:</b> V1
<b>Community</b>	Enter the community string (valid only for version 1 or 2 connections). <b>Default value:</b> public
<b>Timeout (seconds)</b>	Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. <b>Default value:</b> 5
<b>Retries</b>	Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. <b>Default value:</b> 1
<b>Port</b>	Enter the port to use when requesting data from the SNMP agent. <b>Default value:</b> 161
<b>Starting OID</b>	Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered. You should edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value of 1 did not enable retrieving any counters, then you may have to enter a different value. <b>Default value:</b> 1

GUI Element	Description
<b>MIB file</b>	<p>Select either the <b>LOAD-BAL-SYSTEM-MIBS.txt</b> file or <b>All MIBs</b>. Selecting the <b>LOAD-BAL-SYSTEM-MIBS.txt</b> file displays only those objects that are described within that MIB file. Selecting <b>All MIBs</b> displays all objects discovered on the given F5 Big-IP when browsing counters. If no MIB information is available for an object, it is still displayed, but with no textual name or description.</p> <p><b>Default value:</b> All MIBs</p>
<b>Counter calculation mode</b>	<p>Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are:</p> <ul style="list-style-type: none"> <li>▶ <b>Calculate delta.</b> Calculates a simple delta of the current value from the previous value.</li> <li>▶ <b>Calculate rate</b> Calculates a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements.</li> <li>▶ <b>Do not calculate.</b> No calculation is performed.</li> </ul> <p><b>Note:</b> This option only applies to the aforementioned object types. An SNMP by MIB monitor that monitors Counter objects as well as DisplayString objects only performs this calculation on the Counter objects.</p>
<p><b>V3 SNMP Settings</b> (This panel is enabled only if V3 is selected in the SNMP version field)</p>	
<b>SNMP V3 authentication type</b>	<p>Select the type of authentication to use for version 3 connections.</p> <p><b>Default value:</b> MD5</p>
<b>SNMP V3 user name</b>	<p>Enter the user name for version 3 connections.</p>
<b>SNMP V3 authentication password</b>	<p>Enter the authentication password to use for version 3 connections.</p>
<b>SNMP V3 privacy password</b>	<p>Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.</p>



GUI Element	Description
<b>SNMP V3 context engine ID</b>	Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.
<b>SNMP V3 context name</b>	Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.
<b>SNMP Counters</b>	
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ The counters displayed are those received during the timeout period, and may not include all the counters available on the server. Specifying a longer timeout in the <b>Timeout (seconds)</b> field in the SNMP Connection Settings panel may result in receiving more counters. The total time for receiving the counters may be longer than the timeout specified, due to additional processing time not part of the request/response period.</li> <li>▶ Due to third-party counter restrictions, the total number of counters that can be monitored is limited to 32.</li> </ul> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>



# 32

---

## File Monitor

This chapter includes the main concepts and reference information for the File monitor.

### **This chapter includes:**

#### Concepts

- ▶ File Monitor Overview on page 539

#### Reference

- ▶ File Monitor Settings on page 541

### **File Monitor Overview**

The File monitor is useful for watching files that can grow too large and use up disk space, such as log files. Other files that you may want to watch are Web pages that have important content that does not change often.

You can set up your File Monitors to monitor file size, age, or content, and set a threshold at which you should be notified. SiteScope can alert you to unauthorized content changes so that you can correct them immediately. You can write scripts for SiteScope to run that automatically roll log files when they reach a certain size.

The File monitor supports monitoring remote servers running on HP NonStop operating systems.

This section also includes:

- “Reading and Status” on page 540
- “Configuring the Monitor” on page 540

### **Reading and Status**

Each time the File monitor runs, it returns a reading and a status and writes them in the monitoring log file. It also writes the file size and age into the log file.

The reading is the current value of the monitor. Possible values are:

- OK
- content match error
- file not found
- contents changed

An error status is returned if the current value of the monitor is anything other than OK.

### **Configuring the Monitor**

For details on configuring the monitor, see “File Monitor Settings” on page 541.

 **File Monitor Settings**

<b>Description</b>	<p>Use the File monitor to read a specified file and check the size and age of the file. This helps you verify the contents of files by:</p> <ul style="list-style-type: none"> <li>▶ Matching the contents for a piece of text, or by,</li> <li>▶ Checking to see if the contents of the file have changed.</li> </ul> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This monitor supports monitoring remote servers running on HP NonStop operating systems.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “File Monitor Overview” on page 539</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## File Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the file you want to monitor is located. Select a server from the server list (only UNIX remote servers that have been configured in SiteScope and the local SiteScope machine are displayed), or click <b>Add Remote Server</b> to add a new UNIX server.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Add Remote Server</b>	<p>Click to open the Add UNIX Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>

GUI Element	Description
<p><b>File name</b></p>	<p>Enter the path and name to the file you want to monitor. For reading files on remote UNIX machines, the path must be relative to the home directory of the UNIX user account being used to login to the remote machine.</p> <p><b>Example:</b> It may be necessary to provide the full path to the target file, such as <code>/opt/application/logs/user.log</code>.</p> <p>You must also select the corresponding remote UNIX server in the <b>Server</b> box described above. For details on which UNIX user account to use for the applicable remote server, see “Remote Servers Overview” on page 1276.</p> <p>For reading files on remote Windows NT/2000 servers, you use NetBIOS to specify the server and UNC path to the remote log file.</p> <p><b>Example:</b> <code>\\remoteserver\sharedfolder\filename.log</code>.</p> <p>You can also monitor files local to the server where SiteScope is running.</p> <p><b>Example:</b> <code>C:\application\appLogs\access.log</code>.</p> <p>Optionally, you can use regular expressions for special date and time variables to match on log file names that include date and time information.</p> <p><b>Example:</b> You can use a syntax of <code>s/ex\$shortYear\$\$0month\$\$0day\$.log/</code> to match a current date-coded file. For details on using regular expressions and dates, see “SiteScope Date Variables” on page 274.</p>
<p><b>File encoding</b></p>	<p>If the file content to be monitored uses an encoding that is different than the encoding used on server where SiteScope is running, select the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character set used in the target file. This enables SiteScope to match and display the encoded file content correctly.</p> <p><b>Default value:</b> windows-1252</p>

GUI Element	Description
<b>Match content</b>	<p>Enter a string of text to check for in the returned page. If the text is not contained in the page, the monitor displays <b>no match on content</b>. The search is case sensitive. HTML tags are part of a text document, so include them if they are part of the text you are searching for. This works for XML pages as well.</p> <p><b>Example:</b> <code>&lt;B&gt; Hello&lt;/B&gt; World</code></p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p><b>Example:</b> <code>/href=Doc\d+\.\html/</code> or <code>/href=doc\d+\.\html/i</code></p> <p>To save and display a particular piece of text as part of the status, use parentheses in a Perl regular expression.</p> <p><b>Example:</b> <code>/Temperature: (\d+)</code>. This returns the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</p> <p>For details on regular expressions, see “Using Regular Expressions” on page 261.</p> <p>You can also use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</p>



GUI Element	Description
<b>Check for content changes</b>	<p>Unless this is set to "no content checking" (the default) SiteScope records a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs. If the checksum changes, the monitor has a status of "content changed error" and goes into error. If you want to check for content changes, you should use "compare to saved contents".</p> <p>The options for this setting are:</p> <ul style="list-style-type: none"> <li>➤ <b>No content checking</b> (default). SiteScope does not check for content changes.</li> <li>➤ <b>Compare to last contents</b>. The new checksum is recorded as the default after the initial error <b>content changed error</b> occurs, so the monitor returns to OK until the checksum changes again.</li> <li>➤ <b>Compare to saved contents</b>. The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor gets a <b>content changed error</b> and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents.</li> <li>➤ <b>Reset saved contents</b>. Takes a new snapshot of the page and saves the resulting checksum on the first monitor run after this option is chosen. After taking the snapshot, the monitor reverts to <b>compare to saved contents</b> mode.</li> </ul>
<b>No error if file not found</b>	<p>Select if you want this monitor to remain in Good status if the file is not found. The monitor status is Good regardless of how the monitor's thresholds have been configured.</p>



# 33

---

## Formula Composite Monitor

This chapter includes the main concepts and reference information for the Formula Composite monitor.

### **This chapter includes:**

#### Concepts

- ▶ Formula Composite Monitor Overview on page 547

#### Reference

- ▶ Formula Composite Monitor Settings on page 550

### **Formula Composite Monitor Overview**

Use this monitor if you have devices or systems in your network that return values that you want to combine in some way to produce a composite value. The following monitor types can be used to build a Formula Composite monitor:

- ▶ Database Query monitor. For more information see “Database Query Monitor Overview” on page 477.
- ▶ Microsoft Windows Performance Counter monitor. For more information see “Microsoft Windows Performance Counter Monitor Overview” on page 706.
- ▶ Script monitor. For more information see “Script Monitor Overview” on page 833.
- ▶ SNMP monitor. For more information see “SNMP Monitor Overview” on page 882.

If you need alert logic that is more complex than SiteScope's standard alerts allow, you can use the Formula Composite monitor to create custom alert behavior. For example, if you have two parallel network devices that record network traffic but the values need to be combined to produce an overall figure of network traffic. This monitor may also be used to combine the results returned by scripts run on two different machines.

Each time the Formula Composite monitor runs, it returns a status based on the measurement results of the two subordinate monitors and the calculation specified for the composite monitor.

This section includes:

- ▶ “Setup Requirements” on page 548
- ▶ “Notes and Limitations” on page 549
- ▶ “Configuring the Monitor” on page 549

### **Setup Requirements**

- ▶ You must create at least two individual Script, SNMP, Database Query or Microsoft Windows Performance Counter monitor instances before you can set up a Formula Composite monitor for those monitors.
- ▶ The monitors you create for use with a Formula Composite monitor should be configured to return a single value per monitor. This is generally simple with SNMP monitors. Database Query and Script monitors should use queries and scripts that return a single value. For Microsoft Windows Performance Counter monitors, you can use the (Custom Object) option for the **PerfMon Chart File** setting and then specify a single performance **Object**, **Counter**, and **Instance** (if applicable) in the Microsoft Windows Performance Counter Monitor Settings section of the monitor setup. If a subordinate monitor is configured to return more than one numeric measurement, only the first numeric measurement from that monitor instance is used by the Formula Composite monitor.

## Notes and Limitations

- ▶ You should only use the Formula Composite monitor for calculations that you consider to be compatible data types. The monitor does not verify that the data returned by the subordinate monitors are compatible.
- ▶ You can select two different types of monitors as subordinate monitors of a Formula Composite monitor. For example, one monitor may be a Script monitor and the other may be a Database Query monitor.
- ▶ Moving any of the monitors being used by the Formula Composite monitor causes the composite monitor to report an error. If it is necessary to move either of the underlying monitors, recreate or edit the Formula Composite monitor to select the monitor from its new location.

## Configuring the Monitor



For details on configuring the monitor, see “Formula Composite Monitor Settings” on page 550.

## Formula Composite Monitor Settings

<b>Description</b>	<p>Simplifies the monitoring of complex network environments by checking the status readings of two SNMP, Script, Database Query, or Microsoft Windows Performance Counter monitors and performing an arithmetic calculation on their results.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.
<b>Included in Tasks</b>	"Deploy a Monitor – Workflow" on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ "Formula Composite Monitor Overview" on page 547</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 354.</li> </ul>

### Formula Composite Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Monitors</b>	<p>Click the <b>Add</b>  button, and select two SNMP monitors, two Script monitors, two Database monitors, or two Microsoft Windows Performance Counter monitors that the Formula Composite monitor should operate on. Click <b>Add Selected Monitors</b> to display the selected monitors in the Monitors box.</p> <p>To remove monitors from the list, select the monitors and click the <b>Delete</b>  button.</p>

GUI Element	Description
<b>Run monitors</b>	<p>Select if you want the Formula Composite monitor to control the scheduling of the selected monitors, as opposed to just checking their status readings. This is useful if you want the monitors to run one after another or run at approximately the same time.</p> <p><b>Note:</b> Any monitors that are to be run this way should not also be run separately, so set <b>Frequency</b> in Monitor Run Settings to 0. Those monitors then only run when scheduled by the Formula Composite monitor.</p>
<b>Monitor delay (seconds)</b>	<p>If <b>Run monitors</b> is selected, this is the number of seconds to wait between running each monitor.</p> <p><b>Default value:</b> 0 seconds</p>
<b>Operation</b>	<p>Select the arithmetic operation to be performed on the results of the two monitors selected above. You can add the results, multiply the results of the two monitors, subtract the results of the first from the second, divide the second by the first, and so on.</p>
<b>Constant</b>	<p>Enter an operator and a constant to operate on the result of the calculation specified in the <b>Operation</b> item above. For example, if an <b>Operation</b> of Add is selected above, entering the characters *8 in the <b>Constant</b> box multiplies the result of the Add operation by 8. The syntax for this box should be &lt;operator&gt; &lt;number&gt;. Valid operators are + (addition), - (subtraction), * (multiplication), and / (division). Numbers may be integers or decimals.</p>
<b>Result label</b>	<p>Enter a name for the result of the formula calculation.</p>





# 34

---

## FTP Monitor

This chapter includes the main concepts and reference information for the FTP monitor.

### **This chapter includes:**

#### Concepts

- ▶ FTP Monitor Overview on page 553

#### Reference

- ▶ FTP Monitor Settings on page 556

### **FTP Monitor Overview**

If you provide FTP access to files, it is important to check that your FTP server is working properly. Use the FTP monitor to check FTP servers to insure the accessibility of FTP files.

In addition to retrieving specific files, the FTP monitor can help you verify that the contents of files, either by matching the contents for a piece of text, or by checking to see if the contents of the file ever changes compared to a reserve copy of the file.

While you may have many files available for FTP from your site, it is not necessary to monitor every one. We recommend that you check one small file and one large file.

This section contains the following topics:

- “Setup Requirements” on page 554
- “Status” on page 554
- “Scheduling the Monitor” on page 555
- “Configuring the Monitor” on page 555

### **Setup Requirements**

To use this monitor, you must:

- Know the relative paths, if any, to the files on the FTP server.
- Know an applicable user name and password to access the files.
- Know the filenames of one or more files available for FTP transfer.

### **Status**

The reading is the current value of the monitor. Possible values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- login failed
- file not found
- contents changed
- The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

## Scheduling the Monitor

A common strategy is to monitor a small file every 10 minutes or so just to verify that the server is functioning. Then schedule a separate monitor instance to FTP a large file once or twice a day. You can use this to test the ability to transfer a large file without negatively impacting your machine's performance. You can schedule additional monitors that watch files for content and size changes to run every 15 minutes to half hour. Choose an interval that makes you comfortable.

If you have very important files available, you may also want to monitor them occasionally to verify that their contents and size do not change. If the file does change, you can create a SiteScope alert that runs a script to automatically replace the changed file with a back-up file.

## Configuring the Monitor

For details on configuring the monitor, see “FTP Monitor Settings” on page 556.

 **FTP Monitor Settings**

<b>Description</b>	<p>The FTP monitor attempts to log in to an FTP server and retrieve a specified file. A successful file retrieval indicates that your FTP server is functioning properly.</p> <p>Use this page to add a monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>FTP Tool</b> is available when configuring this monitor to access an FTP server and view the interaction between SiteScope and the FTP server (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “FTP Server Tool” on page 208.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “FTP Monitor Overview” on page 553</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## FTP Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Basic FTP Settings</b>	
<b>FTP server</b>	Enter the IP address or the name of the FTP server that you want to monitor. <b>Example:</b> 206.168.191.22 or ftp.thiscompany.com (ftp.thiscompany.com:<port number> to specify a different port)
<b>File</b>	Enter the file name to retrieve from the FTP server. <b>Example:</b> /pub/docs/mydoc.txt You can use a regular expression to insert date and time variables. For details on using SiteScope's special data and time substitution variables in the file path, see "SiteScope Date Variables" on page 274. <b>Example:</b> s/C:\\firstdir\\\$shortYear\$\$0month\$\$0day\$/
<b>User name</b>	Enter the name used to log into the FTP server. A common user name for general FTP access is user name anonymous.
<b>Password</b>	Enter the password used to log into the FTP server. If using the anonymous login, the password is also anonymous.
<b>Passive mode</b>	Select this box if you want SiteScope to use FTP passive mode. You use this mode to enable FTP to work through firewalls.
<b>Advanced FTP Settings</b>	

GUI Element	Description
<b>Match content</b>	<p>Enter a string of text to check for in the returned file. If the text is not contained in the file, the monitor displays <b>no match on content</b>. The search is case sensitive. You may also perform a regular expression match by enclosing the string in forward slashes, with an "i" after the trailing slash indicating case-insensitive matching.</p> <p><b>Example:</b> <code>"/Size \d\d/"</code> or <code>"/size \d\d/i"</code></p>
<b>Check for content changes</b>	<p>SiteScope records a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs. If the checksum changes, the monitor has a status of <b>content changed error</b> and go into error. If you want to check for content changes, you usually want to use compare to saved contents.</p> <p>The options for this setting are:</p> <ul style="list-style-type: none"> <li>▶ <b>No content checking</b> (default). SiteScope does not check for content changes.</li> <li>▶ <b>Compare to last contents</b>. Any changed checksum is recorded as the default after the change is detected initially. Thereafter, the monitor returns to a status of <b>OK</b> until the checksum changes again.</li> <li>▶ <b>Compare to saved contents</b>. The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor gets a <b>content changed error</b> and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents.</li> <li>▶ <b>Reset saved contents</b>. Takes a new checksum of the file and saves the resulting checksum on the first monitor run after this option is chosen. After taking the updated checksum, the monitor reverts to <b>compare to saved contents</b> mode.</li> </ul>

GUI Element	Description
<b>Timeout (seconds)</b>	<p>The number of seconds that the FTP monitor should wait for a file to complete downloading before timing out. Once this time period passes, the FTP monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 60 seconds</p>
<b>Connection timeout (seconds)</b>	<p>The number of seconds that the FTP monitor should wait to connect to the FTP server before timing out. Once this time period passes, the FTP monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 30 seconds</p>
<b>HTTP Proxy Settings</b>	
<b>FTP proxy</b>	<p>You may instruct SiteScope to run the FTP through an HTTP proxy. Generally, if you use an HTTP proxy you have it set up in your browser. Enter that same information here. Remember to include the port.</p> <p><b>Example:</b> proxy.thiscompany.com:8080</p> <p><b>Note:</b> The FTP monitor does not support an FTP Proxy server.</p>
<b>Proxy user name</b>	<p>If the proxy server requires a name and password to access the file, enter the name here. The proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy password</b>	<p>If the proxy server requires a name and password to access the file, enter the password here. The proxy server must support Proxy-Authenticate for these options to function.</p>





# 35

---

## HP NonStop Event Log Monitor

This chapter includes the main concepts and reference information for the HP NonStop Event Log monitor.

### **This chapter includes:**

#### Concepts

- ▶ HP NonStop Event Log Monitor Overview on page 561

#### Reference

- ▶ HP NonStop Event Log Monitor Settings on page 562

### **HP NonStop Event Log Monitor Overview**

Use the HP NonStop Event Log monitor to monitor the Event Logs for added entries on HP NonStop Operating System servers. The HP NonStop Event Log monitor examines events that occurred after the time that the monitor was created. Each time the monitor runs thereafter, it examines only those entries added since the last time it ran. You can choose to filter out messages that are not important by using the boxes listed under Monitor Settings to specify values that must appear in the event entry for the entry to match.

For details on configuring the monitor, see “HP NonStop Event Log Monitor Settings” on page 562.

## HP NonStop Event Log Monitor Settings

<b>Description</b>	<p>The HP NonStop Event Log monitor enables you to monitor Event Logs for added entries on a single HP NonStop Operating System server.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ When configuring this monitor in template mode, you can use regular expressions to define counters.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “HP NonStop Event Log Monitor Overview” on page 561</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## HP NonStop Event Log Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>URL</b>	Enter the URL of the OSM Event Viewer. <b>Example:</b> https://<nonstopserver>:9991
<b>Match content</b>	Enter the text to look for in the log entries. You can also use a regular expression in this entry to match text patterns. The monitor reports how many times the matched pattern was found. To match text that includes more than one line of text, add an s search modifier to the end of the regular expression. For details, see “Using Regular Expressions” on page 261. You can also use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.
<b>Timeout (seconds)</b>	The number of seconds that the monitor should wait for an event before timing-out. Once this time period passes, the monitor logs an error and reports an error status. <b>Default value:</b> 60 seconds
<b>Retries</b>	Enter the number of times that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request for is a recoverable error. <b>Default value:</b> 0
<b>Time zone</b>	Select the appropriate time zone, according to the location of the HP NonStop server.

GUI Element	Description
<b>Filter Settings</b>	
<b>Event sources</b>	<p>Enter the collectors or log file name. You can type more than one collector, separated by comma. Events from multiple collectors are merged by generation time. You can also specify a single event log file.</p> <p><b>Default value:</b> \$ZLOG</p>
<b>Options</b>	<p>Enter filter options. You can enter more than one option, using commas as separators.</p> <p><b>Example:</b> CPU 0, PIN 253</p>
<b>Owner</b>	<p>Enter an owner in this field (up to 8 characters).</p>
<b>Subsystem names</b>	<p>Enter a subsystem name. You can enter more than one subsystem, using commas as separators.</p> <p><b>Example:</b> PATHWAY, TMF</p> <p>You can use the full subsystem name (for example, PATHWAY), an existing abbreviated subsystem name (for example, PWY), or the subsystem number (for example, 8).</p>
<b>Event IDs</b>	<p>Enter an event number to filter on a specific event number. You can enter a single event number, a set of event numbers separated by commas, a range a..b, or a set of ranges separated by commas. Event numbers may be signed. If you specify any event numbers, you can only have one subsystem.</p>
<b>Filter files</b>	<p>Enter filter names. You can enter more than one filter by using commas as separators. You can add more than one filter file, using commas as separators.</p>

GUI Element	Description
<b>Authentication Settings</b>	
<b>Credentials</b>	<p>The user name and password required to access the HP NonStop server. Select the option to use for providing credentials:</p> <ul style="list-style-type: none"> <li>➤ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password in the <b>User name</b> and <b>Password</b> box.</li> <li>➤ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>

GUI Element	Description
<p><b>Pre-emptive authorization</b></p>	<p>Select when the Authorization user name and Authorization password should be sent if SiteScope requests the target URL.</p> <ul style="list-style-type: none"> <li>▶ <b>Use global preference.</b> Select to have SiteScope use the authenticate setting as specified in the Pre-emptive authorization section of the General Preferences page. This is the default value.</li> <li>▶ <b>Authenticate first request.</b> Select to send the user name and password on the first request SiteScope makes for the target URL. <ul style="list-style-type: none"> <li><b>Note:</b> If the URL does not require a user name and password, this option may cause the URL to fail.</li> </ul> </li> <li>▶ <b>Authenticate if requested.</b> Select to send the user name and password on the second request if the server requests a user name and password. <ul style="list-style-type: none"> <li><b>Note:</b> If the URL does not require a user name and password, this option may be used.</li> </ul> </li> </ul> <p>All options use the <b>Authorization user name</b> and <b>Authorization password</b> entered for this monitor instance. If these are not specified for the individual monitor, the <b>Default authentication user name</b> and <b>Default authentication password</b> specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p><b>Note:</b> Pre-emptive authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
<p><b>Client side certificate</b></p>	<p>If you need to use a client side certificate to access the target URL, select the certificate file using the drop down menu. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You enter the password for the certificate in the <b>Client side certificate password</b> box.</p> <p><b>Note:</b> Client side certificate files must be copied into the <b>&lt;SiteScope root directory&gt;\templates.certificates</b> directory.</p>

GUI Element	Description
<b>Client side certificate password</b>	If you are using a client side certificate and that certificate requires a password, enter the password.
<b>Accept untrusted certificates for HTTPS</b>	Select this option if you need to use certificates that are untrusted in the certificate chain to access the target URL using Secure HTTP (HTTPS). <b>Default value:</b> Not selected
<b>Accept invalid certificates for HTTPS</b>	Select this option if you need to accept an invalid certificate to access the XML URL using Secure HTTP (HTTPS). This may happen, for example, if the current date is not in the date ranges specified in the certificate chain. <b>Default value:</b> Not selected
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	A proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.
<b>Proxy server user name</b>	If the proxy server requires a name and password to access the URL, enter the name here. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	If the proxy server requires a name and password to access the URL, enter the password here. <b>Note:</b> Your proxy server must support Proxy-Authentication for these options to function.





# 36

---

## HP NonStop Resources Monitor

This chapter includes the main concepts and reference information for the HP NonStop Resources monitor.

### **This chapter includes:**

#### Concepts

- ▶ HP NonStop Resources Monitor Overview on page 569

#### Reference

- ▶ HP NonStop Resources Monitor Settings on page 571

### **HP NonStop Resources Monitor Overview**

Use the HP NonStop Resources monitor to monitor the server system statistics on HP NonStop Operating System servers. You can monitor multiple parameters or measurements with a single monitor instance. This enables you to monitor the remote server for loading, performance, and availability at a basic system level. Create a separate HP NonStop Resources monitor instance for each HP NonStop Operating System server in your environment.

The HP NonStop Resources monitor queries the list of HP NonStop Servers currently configured in the UNIX Remote Servers container. To monitor a remote HP NonStop Operating System server, you must define a NonStop Remote connection profile for the server before you can add an HP NonStop Resources monitor for that server. For details on configuring a remote server, see “Remote Servers Overview” on page 1276.

You can also use the Directory, Disk Space, File, Log File, and Script monitors to monitor remote servers running on HP NonStop Operating Systems. Monitors that do not depend on a remote operating system, such as FTP, Port, SNMP, SNMP by MIB, and URL family monitors, can also support monitoring on an HP NonStop operating system server.

This section includes:

- “Setup Requirements and User Permissions” on page 570
- “Troubleshooting and Limitations” on page 570
- “Configuring the Monitor” on page 571

### **Setup Requirements and User Permissions**

To enable monitoring of remote servers running on a HP NonStop Operating System (using either the HP NonStop Resources monitor or the Directory, Disk Space, File, Log File, or Script monitor), you must perform the following on the HP NonStop Operating System server:

- Create a user for SiteScope monitoring.
- In the `/etc/profile` and `.profile` files, comment out the following string:  
`set -o vi`
- Set the following parameter: `export PS1='$PWD:`

### **Troubleshooting and Limitations**

When configuring a remote server for monitoring the HP NonStop server, if the remote server gives a choice of TACL shell only, select the remote server in **Remote Servers > UNIX Remote Servers**, and enter the following in the **Main Settings** panel:

- In the **Shell name** field, enter `tacl`.
- In the **Login prompt** field, enter `>`.
- In the **Secondary response** field, enter `OSH`.
- In the **User name** box in the **Credentials** section, enter the user name in the format: `logon <user_name>`.

## Configuring the Monitor



For details on configuring the monitor, see “HP NonStop Resources Monitor Settings” on page 571.

### HP NonStop Resources Monitor Settings

<b>Description</b>	<p>The HP NonStop Resources monitor enables you to monitor multiple system statistics on a single HP NonStop Operating System server. The error and warning thresholds for the monitor can be set on one or more server system statistics.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ When configuring this monitor in template mode, you can use regular expressions to define counters.</li> <li>▶ The performance objects and counters available for the HP NonStop Resources monitor vary depending on what operating system options and applications are running on the remote server.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “HP NonStop Resources Monitor Overview” on page 569</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 358.</li> </ul>

## HP NonStop Resources Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the resources you want to monitor are located. Select a server from the server list (only UNIX remote servers that have been configured in SiteScope to run on an HP NonStop operating system are displayed), or click <b>Add Remote Server</b> to add a UNIX server.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p>
<b>Add Remote Server</b>	<p>Click to open the Add UNIX Remote Server dialog box, and enter the configuration details (in the <b>Operating System</b> list, you must select <b>NonStopOS</b>). For details on the user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1302.</p>
<b>Available Counters</b>	<p>Displays the available measurements for this monitor. For each measurement, select the <b>Objects</b>, <b>Instances</b> and <b>Counters</b> you want to check with the HP NonStop Resources monitor, and click the <b>Add Selected Counters</b>  button. The selected measurements are moved to the Selected Counters list.</p>
<b>Selected Counters</b>	<p>Displays the measurements currently selected for this monitor, and the total number of selected counters.</p> <p>To remove measurements selected for monitoring, select the required measurements, and click the <b>Remove Selected Counters</b>  button. The measurements are moved to the Available Counters list.</p>

# 37

---

## IPMI Monitor

This chapter includes the main concepts and reference information for the IPMI monitor.

**This chapter includes:**

**Concepts**

- ▶ IPMI Monitor Overview on page 574

**Reference**

- ▶ IPMI Monitor Settings on page 575

## IPMI Monitor Overview

The Intelligent Platform Management Interface (IPMI) provides an interface for reporting on device operations, such as whether fans are turning and voltage flowing within server hardware. You use the IPMI monitor to monitor server and network element platforms to get a more complete view of component health and operation statistics for IPMI enabled devices running version 1.5.

You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch key operational factors that can seriously effect availability and degrade performance. Create a separate monitor instance for each server you are running.

This section also includes:

- ▶ “Setup Requirements” on page 574
- ▶ “Configuring the Monitor” on page 574

### **Setup Requirements**

The following are requirements for using the IPMI monitor:

- ▶ The device you want to monitor has to be IPMI-enabled. In most cases, this means that the device must be designed for IPMI sensing and include a separate, dedicated IPMI network adapter. The monitor supports IPMI version 1.5 only.
- ▶ You must know the IP address of the IPMI network adapter for the device you want to monitor. In many cases, this IP address is different than the IP address used for other network communication to and from the device. Use an applicable IPMI utility to query for the IP address or contact the applicable system administrator.

### **Configuring the Monitor**

For details on configuring the monitor, see “IPMI Monitor Settings” on page 575.

## IPMI Monitor Settings

<b>Description</b>	<p>Monitors component health and operation statistics for Intelligent Platform Management Interface (IPMI) enabled devices running version 1.5.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “IPMI Monitor Overview” on page 574</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## IPMI Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server name</b>	Enter the IPMI server name or IP address of the IPMI network adapter. <b>Note:</b> The IP address is normally not the same as the ordinary ethernet NIC adapter address.
<b>Port number</b>	Enter the port number of the IPMI device. <b>Default value:</b> 623
<b>Credentials</b>	Select the option for providing the user name and password to be used to access the IPMI server. <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor. <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.



# 38

---

## JMX Monitor

This chapter includes the main concepts and reference information for the JMX monitor.

### **This chapter includes:**

#### Concepts

- ▶ JMX Monitor Overview on page 577

#### Reference

- ▶ JMX Monitor Settings on page 582

### **JMX Monitor Overview**

Use the JMX monitor to monitor performance statistics of Java-based applications that provide access to their statistics by using the standard JMX remoting technology defined by JSR 160 (remote JMX). This monitor supports monitoring on WebLogic 9.x and WebLogic 10.0 - 10.2, Apache Tomcat 5.0, Oracle 10.1.3gAS, and JBoss 4.0.3 servers.

You can monitor multiple parameters or counters with a single monitor instance. The counters available vary from application to application, but normally include both basic JVM performance counters as well as counters specific to the application. You may create one JMX monitor instance for each application you are monitoring, or several monitors for the same application that analyze different counters.

---

**Note:** WebLogic 9.x and WebLogic 10.0 - 10.2 servers can be monitored using a JMX monitor only. For details on how to monitor a WebLogic 9.x or WebLogic 10.0 - 10.2 server, see “Creating a JMX Monitor for a WebLogic 9.x or WebLogic 10.0 - 10.2 Server” on page 580.

---

This section contains the following topics:

- ▶ “Applications Supporting JSR 160” on page 578
- ▶ “Creating a JMX Monitor for a WebLogic 9.x or WebLogic 10.0 - 10.2 Server” on page 580
- ▶ “WebLogic Application Server Topology Settings” on page 580
- ▶ “Troubleshooting and Limitations” on page 581
- ▶ “Configuring the Monitor” on page 581

## **Applications Supporting JSR 160**

Here are some applications that currently support JSR 160 and information about how to monitor them:

- ▶ BEA WebLogic 9.x and WebLogic 10.0 - 10.2 supports JSR 160, which can be enabled on the WebLogic application server by following instructions found on the BEA Web site (<http://e-docs.bea.com/wls/docs90/ConsoleHelp/taskhelp/channels/EnableAndConfigureIOP.html>).

Once enabled, the JMX URL for monitoring the server follows the following form:

```
service:jmx:iiop:///jndi/iiop://<host>:<port>/weblogic.management.mbeanservers.runtime
```

where <host> is the server name or IP address that is running your WebLogic application.

For instructions to create a JMX monitor for WebLogic 9.x and WebLogic 10.0 - 10.2 servers, see “Creating a JMX Monitor for a WebLogic 9.x or WebLogic 10.0 - 10.2 Server” on page 580.

- ▶ Tomcat 5.x supports JSR 160, by defining the following properties to the JVM on startup:
  - ▶ `Dcom.sun.management.jmxremote`
  - ▶ `Dcom.sun.management.jmxremote.port=9999`
  - ▶ `Dcom.sun.management.jmxremote.ssl=false`
  - ▶ `Dcom.sun.management.jmxremote.authenticate=false`

The above properties specify the port as 9999. This value can be changed to any available port. Also, it specifies no authentication. If authentication is necessary, see the Java Sun Web site for more details (<http://java.sun.com/j2se/1.5.0/docs/guide/jmx/tutorial/security.html>). If the above properties are defined when starting Tomcat 5.x on <host>, the following would be the JMX URL for monitoring it:

```
service:jmx:rmi:///jndi/rmi://<host>:9999/jmxrmi
```

---

**Note:** SiteScope 8.x runs within Tomcat 5.x, and can be monitored as described above.

---

- ▶ Other vendors that have released versions of their software that are JSR 160 compliant, include JBoss, Oracle 10g, and IBM WebSphere.

You can find more information about JSR 160 on the Java Community Process Web site (<http://www.jcp.org/en/jsr/detail?id=160>).

## Creating a JMX Monitor for a WebLogic 9.x or WebLogic 10.0 - 10.2 Server

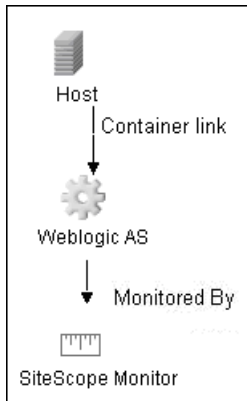
WebLogic 9.x and WebLogic 10.0 - 10.2 servers cannot be monitored using a WebLogic monitor. To monitor a WebLogic 9.x or WebLogic 10.0 - 10.2 server, create a JMX monitor, and enter the following in the **JMX URL** box:

```
service:jmx:iiop:///jndi/iiop://<server_name>:7001/weblogic.management.mbean  
servers.runtime.
```

To help you to select the counters that you require, you can open a WebLogic monitor for versions prior to WebLogic 9.x (WebLogic 6.x, 7.x, and 8.x) and see the counters that were defined there. Search for these same counters in the counter tree. You can select additional counters that are available in the JMX monitor and were not available in the WebLogic monitors.

## WebLogic Application Server Topology Settings

The JMX monitor can identify the topology of WebLogic Application Servers. If **Include topology data when reporting to BAC** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



---


**Note:** The JMX monitor can report topology data to Business Availability Center only when monitoring the WebLogic application server, not when monitoring any other environment.

---

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160 in the HP Business Availability Center Documentation Library.

## Troubleshooting and Limitations

**Problem:** When using the JMX monitor to monitor performance statistics on a JBoss server, the **Good** status is displayed in the SiteScope Dashboard even when the JBoss server is unavailable. SiteScope handles the exceptions differently according to the platform.

- On Windows, each counter is set to **n/a**.
- On Linux and Solaris platforms, the counters are not reset, but the **no data** value is set (and **No Data Availability**  is displayed on the Dashboard).

**Resolution:** A workaround when monitoring JBoss is to change the monitor's properties in Threshold Settings, by setting **If unavailable** to **Set monitor status to error**.

## Configuring the Monitor

For details on configuring the monitor, see “JMX Monitor Settings” on page 582.

## JMX Monitor Settings

<b>Description</b>	<p>Allows you to monitor the performance statistics of those Java-based applications that provide access to their statistics by using the standard JMX remoting technology.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “JMX Monitor Overview” on page 577</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### JMX Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>JMX URL</b>	<p>The URL to gather JMX statistics. Typically the URL begins with <code>service:jmx:rmi:///jndi</code>, followed by information specific to the application.</p> <p><b>Note:</b> When creating a JMX monitor for a WebLogic 9.x or 10.x server, enter the following URL:  <code>service:jmx:iiop:///jndi/iiop://&lt;host&gt;:&lt;port&gt;/weblogic.management.mbeanservers.runtime</code></p>

GUI Element	Description
<b>Domain filter</b>	Domain filter to show only those counters existing within a specific domain (optional).
<b>User name</b>	User name for connection to the JMX application (optional).
<b>Password</b>	Password for connection to the JMX application (optional).
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters. When the server being monitored is a WebLogic 9.x or 10.x server, see “Creating a JMX Monitor for a WebLogic 9.x or WebLogic 10.0 - 10.2 Server” on page 580 for further details.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.  <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.





# 39

---

## LDAP Monitor

This chapter includes the main concepts and reference information for the LDAP monitor.

### **This chapter includes:**

#### Concepts

- ▶ LDAP Monitor Overview on page 585

#### Reference

- ▶ LDAP Monitor Settings on page 587

### **LDAP Monitor Overview**

If your LDAP server is not working properly, the user is not able to access and update information in the directory. Most importantly, the user is not able to perform any authentication using the LDAP server. Use the LDAP monitor to monitor the availability and proper functioning of your LDAP server. Another reason to monitor the LDAP server is so that you can find performance bottlenecks. If your end user and LDAP times are both increasing at about the same amount, the LDAP server is probably the bottleneck.

The most important thing to monitor is the authentication of a specific user on the LDAP server. If more than one LDAP server is used, you should monitor each of the servers. You may also want to monitor round trip time of the authentication process.

This section also includes:

- “Status” on page 586
- “Configuring the Monitor” on page 586

## **Status**

Each time the LDAP monitor runs, it returns a status based on the time it takes to perform the connection.

The possible values for the LDAP status are:

- OK
- warning
- error

An error status or warning status is returned if the current value of the monitor is anything other than OK. Errors occur if SiteScope is unable to connect, receives an unknown host name error, or the IP address does not match the host name.

## **Configuring the Monitor**

For details on configuring the monitor, see “LDAP Monitor Settings” on page 587.

 **LDAP Monitor Settings**

<b>Description</b>	<p>Verifies that a Lightweight Directory Access Protocol (LDAP) server is working correctly by connecting to it and performing a simple authentication. Optionally, it can check the result for expected content.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>LDAP Authentication Tool</b> is available when configuring this monitor to test an LDAP server can authenticate a user by performing a simple authentication (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “LDAP Authentication Tool” on page 211.</li> </ul>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “LDAP Monitor Overview” on page 585</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## LDAP Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Authentication Settings</b>	
<b>LDAP service provider</b>	Enter the constant that holds the name of the environment property for specifying configuration information for the service provider to use. The value of the property should contain a URL string (for example, <code>ldap://somehost:389</code> ). This property may be specified in the environment, an applet parameter, a system property, or a resource file. If it is not specified in any of these sources, the default configuration is determined by the service provider.
<b>Security principal</b>	Enter the constant that holds the name of the environment property for specifying the identity of the principal for authenticating the caller to the service. The format of the principal depends on the authentication scheme. If this property is unspecified, the behavior is determined by the service provider. This should be of the form <code>uid=testuser,ou=TEST,o=mydomain.com</code> .
<b>Security credential</b>	Enter the constant that holds the name of the environment property for specifying the credentials of the principal for authenticating the caller to the service. The value of the property depends on the authentication scheme. For example, it could be a hashed password, clear-text password, key, certificate, and so on. If this property is unspecified, the behavior is determined by the service provider.

GUI Element	Description
<b>LDAP Settings</b>	
<b>Content match</b>	<p>Enter a string of text to check for in the query result. If the text is not contained in the result, the monitor displays no match on content. The search is case sensitive.</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p><b>Example:</b> <code>/href=Doc\d+\.html/</code> or <code>/href=doc\d+\.html/i</code></p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression.</p> <p><b>Example:</b> <code>/Temperature: (\d+)</code>. This would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</p>

GUI Element	Description
<b>Object query</b>	<p>Use this box to enter an object query to look at a LDAP object other than the default user <b>dn</b> object. For example, enter the mail object to check for an email address associated with the dn object entered above. You must enter a valid object query in this text box if you are using a LDAP filter (see the description below).</p> <p><b>Note:</b> To use LDAP version 3 for a particular monitor, type [LDAP-3] before the query. If you want to use version 2 and version 3, type [LDAP-ANY].</p>
<b>LDAP filter</b>	<p>Enter an LDAP filter in this text box to perform a search using a filter criteria.</p> <p>The LDAP filter syntax is a logical expression in prefix notation meaning that logical operator appears before its arguments. For example, the item <code>sn=Freddie</code> means that the <code>sn</code> attribute must exist with the attribute value equal to <code>Freddie</code>.</p> <p>Multiple items can be included in the filter string by enclosing them in parentheses (such as <code>sn=Freddie</code>) and combined using logical operators such as the <code>&amp;</code> (the ampersand conjunction operator) to create logical expressions.</p> <p><b>Example:</b> The filter syntax <code>(&amp; (sn=Freddie) (mail=*))</code> requests LDAP entries that have both a <code>sn</code> attribute of <code>Freddie</code> and a <code>mail</code> attribute.</p> <p>More information about LDAP filter syntax can be found at <a href="http://www.ietf.org/rfc/rfc2254.txt">http://www.ietf.org/rfc/rfc2254.txt</a> and also at <a href="http://java.sun.com/products/jndi/tutorial/basics/directory/filter.html">http://java.sun.com/products/jndi/tutorial/basics/directory/filter.html</a>.</p>

# 40

---

## Link Check Transaction Monitor

This chapter includes the main concepts and reference information for the Link Check monitor.

### **This chapter includes:**

#### Concepts

- ▶ Link Check Monitor Overview on page 591

#### Reference

- ▶ Link Check Monitor Settings on page 592

### **Link Check Monitor Overview**

Use the Link Check monitor to check the internal and external links on a Web page to insure that they can be reached. Each time the Link Check monitor runs, it returns a status and writes it in a link report log file named LinkReport\_<group name><number>.log (this should not be confused with the daily logs). It also writes the total number of link errors, the total number of links, the total number of graphics, and the average time for retrieving a page.

You should monitor the Web site for the availability of key content. This includes checking that image files and linked HTML files are accessible as referenced within the Web pages. Starting with your home page, the Link Check monitor branches out and checks every link available on your entire site by default. If you only want it to check a portion of your site, specify the URL that links into the targeted area. You can limit the number of linked hops the monitor follows in the **Maximum hops** box of the Monitor Settings panel.

You probably only need to run the link monitor once a day to check for external links that have been moved or no longer work and internal links that have been changed. You can also run it on demand any time you do a major update of your Web site.

For details on configuring the monitor, see “Link Check Monitor Settings” on page 592.

## Link Check Monitor Settings

<b>Description</b>	<p>Checks the internal and external links on a Web page to insure that they can be reached. SiteScope begins checking links from a URL that you specify, verifies that linked graphics can be found, and follows HREF links to the referenced URLs. The monitor can be configured to check all of the links on your site or to check a limited number of hops from the initial URL.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Link Check Monitor Overview” on page 591</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>



## Link Check Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>URL</b>	<p>Enter the URL that is the starting point for checking links. The link monitor retrieves the page for this URL and reads the URLs for any links on the page. It continues until it has checked all of the links on the site. Links to other servers are checked but it does not continue and check all the links of those other servers.</p> <p><b>Example:</b> http://demo.thiscompany.com</p>
<b>Search external links</b>	<p>Select to have the monitor follow all links on each page and not just links that contain the original base URL.</p> <p><b>Warning:</b> Using this option may greatly increase the number of links that are tested and the amount of time required for the monitor to run. In some cases this may cause the monitor to run for more than 24 hours without being able to complete all of the link checks. If you select this option, be sure to limit the total number of links to test using the <b>Maximum links</b> setting and limit the depth of the search using the <b>Maximum hops</b> setting.</p> <p><b>Default value:</b> Not selected</p>
<b>Pause (milliseconds)</b>	<p>The delay, in milliseconds, between each link check. Larger numbers lengthen the total time to check links but decrease the load on the server.</p> <p><b>Default value:</b> 250 milliseconds</p>
<b>Timeout (seconds)</b>	<p>The number of seconds that the URL monitor should wait for a page to begin downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 60 seconds</p>

GUI Element	Description
<b>Maximum links</b>	<p>The maximum number of links this monitors checks. When the maximum number of links is reached the monitor stops and reports the results of those links that were checked. Increase this number if you have a large site and want to check every link on the site.</p> <p><b>Default value:</b> 800</p>
<b>Maximum hops</b>	<p>The maximum number of internal links that SiteScope should follow from the starting URL. Limiting the number of links reduces the number of URLs that SiteScope follows and shortens the time to complete the report. SiteScope does not follow any links on external pages. Select one of the predefined choices using the <b>Commonly used values</b> list. To enter your own limit, enter a numeric value in the <b>Other values</b> box.</p> <p><b>Default value:</b> Main page links</p> <p><b>Example:</b> If you set the number of hops to 3, SiteScope checks all internal pages that can be reached within 3 links from the starting URL.</p>
<b>POST data</b>	<p>Enter any form values required for the first page being checked. This is useful if you need to log in using an HTML form to reach the rest of the site that you are checking. Enter form values in the format key=value (one on each line).</p>
<b>Authorization Settings</b>	
<b>Authorization user name</b>	<p>If the URL specified requires a user name for access, enter the name.</p>
<b>Authorization password</b>	<p>If the URL specified requires a password for access, enter the password.</p>
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	<p>Optionally, a proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.</p>

GUI Element	Description
<b>Proxy server user name</b>	If the proxy server requires a name to access the URL, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	If the proxy server requires a password to access the URL, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.



# 41

---

## Log File Monitor

This chapter includes the main concepts and reference information for the Log File monitor.

### **This chapter includes:**

#### Concepts

- ▶ Log File Monitor Overview on page 597

#### Reference

- ▶ Log File Monitor Settings on page 600

### **Log File Monitor Overview**

The Log File monitor watches for specific entries added to a log file by looking for entries containing a text phrase or a regular expression. You can use it to automatically scan log files for error information. With SiteScope doing this for you at set intervals, you can eliminate the need to scan the logs manually. In addition, you can be notified of warning conditions that you may have otherwise been unaware of until something more serious happened.

By default, each time that SiteScope runs this monitor, it starts from the point in the file where it stopped reading last time it ran. This insures that you are notified only of new entries and speeds the rate at which the monitor runs. You change this default behavior using the **Check from beginning** property. For details, see “Check from beginning” on page 603.

The Log File monitor supports monitoring remote servers running on HP NonStop operating systems.

---

**Note:** Monitoring log files using SSH on Windows platforms is supported from SiteScope version 8.5 and later.

---

This section contains the following topics:

- “Setup Requirements and User Permissions” on page 598
- “Scheduling the Monitor” on page 598
- “Customizing Log File Content Matches and Monitor Alerts” on page 599
- “Configuring the Monitor” on page 599

### **Setup Requirements and User Permissions**

The following configuration requirements must be performed or verified before the Log File monitor can be used:

- The log file to be monitored must exist, and be accessible under credentials used for connecting to the remote server, or under which SiteScope is running (if monitoring a local file).
- The remote server should be created with credentials that grant read access on the monitored file.

### **Scheduling the Monitor**

You can schedule your Log File Monitors to run as often as every 15 seconds. However, depending on the size of the log file, the total number of monitors you have running, and **Check from beginning** option selected, the monitor may take 15 seconds or longer to check the file for the desired entries. The default update schedule of every 10 minutes is a reasonable frequency in most cases.

## Customizing Log File Content Matches and Monitor Alerts

You can create a Log File monitor that triggers customized alerts for content matches according to the threshold status of the monitor.

**To configure the Log File monitor with custom matches and alerts:**

- 1** In the Log Monitor Settings, configure the following settings:
  - ▶ **Run Alerts:** Select the **For each log entry matched** option.
  - ▶ **Content match:** Enter the text to look for in the log entries. For example, to find text entries `redflag` and `disaster` in the log file, enter `/(redflag|disaster)/`.
  - ▶ **Match value label:** Enter a label name for the matched values found in the target log file. For example, type `matchedValue`.
- 2** In the Threshold Settings, set the error and warning threshold. For example, set `Error if matchedValue == disaster` and set `Warning if matchedValue == redflag`.
- 3** Configure error, warning, and good alerts for the Log File monitor. The alert that is sent depends on the threshold that is met for each entry matched. For example, if the error threshold is met, the error alert is triggered. For details on configuring alerts, see “Configure an Alert” on page 1984.

## Configuring the Monitor

For details on configuring the monitor, see “Log File Monitor Settings” on page 600.

 **Log File Monitor Settings**

<b>Description</b>	<p>The Log File monitor checks for specific entries added to a log file by looking for entries containing a text phrase or a regular expression.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This monitor supports monitoring remote servers running on HP NonStop operating systems.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Log File Monitor Overview” on page 597</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>



## Log File Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>Server</b>	<p>The server where the file you want to monitor is located. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> If using NetBIOS to connect to other servers in an NT domain, use the UNC format to specify the path to the remote log file.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>➤ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>➤ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>

GUI Element	Description
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>
<b>Log file path</b>	<p>Enter the path to the log file you want to monitor.</p> <ul style="list-style-type: none"> <li>▶ For reading log files on remote UNIX machines, the path must be relative to the home directory of the UNIX user account being used to log in to the remote machine.</li> <li>▶ For reading log files on remote Windows NT/2000 servers using the NetBIOS method, use UNC to specify the path to the remote log file. <b>Example:</b> \\remoteserver\sharedfolder\filename.log</li> <li>▶ For reading log files on remote Windows NT/2000 servers using the SSH method, specify the local path of the remote log file on the remote machine. <b>Example:</b> C:\Windows\System32\filename.log</li> </ul> <p>You must also select the corresponding remote Windows SSH server in the <b>Servers</b> box. For details on configuring a remote Windows server for SSH, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p> <p>You can also monitor files local to the server where SiteScope is running. <b>Example:</b> C:\application\appLogs\access.log</p> <p>Optionally, you can use special date and time regular expression variables to match log file names that include date and time information. For example, you can use a syntax of s/ex\$shortYear\$\$0month\$\$0day\$.log/ to match a current date-coded log file. For details on using regular expressions, refer to “SiteScope Date Variables” on page 274.</p>

GUI Element	Description
<b>Run alerts</b>	<p>Select the method for running alerts for this monitor.</p> <ul style="list-style-type: none"> <li>▶ If the <b>For each log entry matched</b> option is chosen, the monitor triggers alerts for every matching entry found. When the Log File monitor is run, the monitor never reports a status of error or warning, regardless of the results of the content match. For details on how to create a Log File monitor that triggers customized alerts for content matches, see “Customizing Log File Content Matches and Monitor Alerts” on page 599.</li> <li>▶ If the <b>Once, after all log entries have been checked</b> option is chosen, then the monitor counts up the number of matches and then triggers alerts.</li> </ul> <p><b>Note:</b> The status category is resolved according to the last content that matched the regular expression. If the last matched content does not meet the threshold measurement, an alert is not triggered.</p>
<b>Check from beginning</b>	<p>Select the file checking option for this monitor instance. This setting controls what SiteScope looks for and how much of the target file is checked each time that the monitor is run.</p> <ul style="list-style-type: none"> <li>▶ <b>Never.</b> Checks newly added records only.</li> <li>▶ <b>First time only.</b> Checks the whole file once, and then newly added records only.</li> <li>▶ <b>Always.</b> Always checks the whole file.</li> </ul> <p><b>Default value:</b> Never</p>

GUI Element	Description
<b>Content match</b>	<p>Enter the text to look for in the log entries. You can also use a regular expression in this entry to match text patterns. Unlike the content match function of other SiteScope monitors, the Log File monitor content match is run repeatedly against the most recent content of the target log file until all matches are found. This means the monitor not only reports if the match was found but also how many times the matched pattern was found. To match text that includes more than one line of text, add an s search modifier to the end of the regular expression. For details, see “Using Regular Expressions” on page 261.</p> <p><b>Note:</b> If you enter more than four values here, when you create a report by clicking the monitor title, the report includes only the first four values.</p>
<b>Open Tool</b>	<p>Click to open the Regular Expression Tool, which enables you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see “Regular Expression Tool” on page 232.</p>
<b>Advanced Settings</b>	
<b>Log file encoding</b>	<p>If the log file content to be monitored uses an encoding that is different than the encoding used on server where SiteScope is running, select the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the target log file. This enables SiteScope to match and display the encoded log file content correctly.</p> <p><b>Default value:</b> windows-1252</p>

GUI Element	Description
<b>Rules file path</b>	<p>In rare cases, it may be necessary to create a custom rules file to specify the log entries to match and the alerts to send. An example rules file is located in &lt;SiteScope root directory&gt;\conf\examples\sample.rules. Make a copy of this file and rename. There is no required naming convention. Open the file with the editor of your choice, and using the comments as a guideline, edit the file to meet your needs. When you are finished, enter the full path to your rules file.</p>
<b>Match value labels</b>	<p>Use this option to enter labels for the matched values found in the target log file. The match value labels are used as variables to access retained values from the <b>Content match</b> expression for use with the monitor threshold settings. Separate multiple labels with a comma (.). The labels are used to represent any retained values from the <b>Content match</b> regular expression in the parameters available for the status threshold settings (Error if, Warning if, and Good if). These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.</p> <p><b>Note:</b> If you enter more than four match value labels, when you create a report by clicking the monitor title, the report includes only the first four values.</p>
<b>Multi-line match</b>	<p>Select to run a regular expression match on multiple lines of text.</p> <p><b>Default value:</b> Not selected</p>

GUI Element	Description
<b>Server-side processing</b>	<p>Select to process log file data on the server-side. Benefits include low memory usage and low CPU utilization on the SiteScope server, and faster monitor run. Server-side processing does however cause high CPU utilization on the remote server when processing the file.</p> <p><b>Default value:</b> Not selected (we recommend using this option only if SiteScope performance is affected by large amounts of data being appended to the target log file between monitor runs, and the Log File monitor is performing badly in regular mode).</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ Server-side processing is enabled for remote Linux, RedHat Enterprise Linux, and Sun Solaris servers only. Windows SSH is not supported.</li> <li>▶ “Rule files” are not supported in this mode.</li> <li>▶ The encoding for the remote server must be Unicode, or match the encoding of the log file (if the remote file is in Unicode charset).</li> </ul>
<b>No error if file not found</b>	<p>Select if you want this monitor to remain in Good status if the file is not found. The monitor status remains Good regardless of the monitor threshold configuration.</p> <p><b>Default value:</b> Not selected</p>

# 42

---

## Mail Monitor

This chapter includes the main concepts and reference information for the SAP Work Processes monitor.

### **This chapter includes:**

#### Concepts

- ▶ Mail Monitor Overview on page 607

#### Reference

- ▶ Mail Monitor Settings on page 608

### Mail Monitor Overview

The Mail monitor checks that the mail server is accepting requests, and also verifies that a message can be sent and retrieved. It does this by sending a standard mail message using SMTP and then retrieving that same message by using a POP user account. Each message that SiteScope sends includes a unique key that it checks to insure that it does not retrieve the wrong message and return a false OK reading. Each time the Mail monitor runs, it returns a status and writes it in the log file. It also writes the total time it takes to send and receive the mail message in the log file. If SiteScope is unable to complete the entire loop, it generates an error message.

We recommend that you monitor your primary mail server at least every five minutes. The other mail servers can be monitored less frequently. You may find it useful to set up a special mail account to receive the test email messages send by SiteScope.

For details on configuring the monitor, see “Mail Monitor Settings” on page 608.

## Mail Monitor Settings

<p><b>Description</b></p>	<p>The Mail monitor checks to see that the mail server is both accepting and delivering messages. Use this monitor to verify that all your mail servers, including internal servers where a firewall is used, are working properly.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>➤ Monitors must be created in a group in the monitor tree.</li> <li>➤ The <b>Mail Round Trip Tool</b> is available when configuring this monitor to verify that the mail server is accepting requests and that a message can be sent and retrieved (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Mail Round Trip Tool” on page 214.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ “Mail Monitor Overview” on page 607</li> <li>➤ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>



## Mail Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Action</b>	<p>Select the action the Mail monitor should take with respect to the mail server:</p> <ul style="list-style-type: none"> <li>▶ <b>Send and receive.</b> This option enables you to send a test message to an SMTP server and then to receive it back from the POP3 or IMAP4 server. This checks that the mail server is up and running.</li> <li>▶ <b>Receive only.</b> This option enables you to check the incoming POP3 or IMAP4 mail servers for a message that was sent previously. This check is done by matching the content of the previously sent message. <b>Note:</b> If the this option is selected, the <b>Match content</b> box must have a value to match against. Also, if this option is selected, you should use this monitor for a dedicated mail account that is not being accessed by any other mail client. If another mail client attempts to retrieve mail messages from the account that the Mail monitor is monitoring in <b>Receive only</b> mode, the monitor and the other mail client may lock each other out of the account, and neither is able to retrieve the messages.</li> <li>▶ <b>Send only.</b> This option checks that the receiving mail server has accepted the message.</li> </ul>
<b>Sending email server (SMTP)</b>	<p>Enter the host name of the SMTP mail server to which the test mail message should be sent.</p> <p><b>Example:</b> mail.thiscompany.com</p>
<b>Send to address</b>	<p>Enter the mail address to which the test message should be sent.</p>
<b>Receiving protocol</b>	<p>Select the protocol used by the receiving mail server. You use the POP3 option to check the POP3 mail server for a sent message. You use the IMAP4 option to check the IMAP mail server for a sent message.</p>

GUI Element	Description
<p><b>Receiving email server</b></p>	<p>Enter the host name of the POP3/IMAP4 mail server that should receive the test message. This can be the same mail server to which the test message was sent.</p> <p><b>Example:</b> mail.thiscompany.com</p>
<p><b>Receiving email server user name</b></p>	<p>Enter a POP user account name on the receiving mail server. A test email message is sent to this account and the Mail monitor logs in to the account and verifies that the message was received. No other mail in the account is touched; therefore you can use your own personal mail account or another existing account for this purpose.</p> <p><b>Example:</b> support</p> <p><b>Note:</b> If you use a mail reader that automatically retrieves and deletes messages from the server, there is a chance that the Mail monitor won't see the mail message and therefore reports an error.</p>
<p><b>Receiving email server password</b></p>	<p>Enter a password, if necessary, for the receiving mail account.</p>

GUI Element	Description
<p><b>Receive only content match</b></p>	<p>Enter a string of text to match against the contents of the incoming message. If the text is not contained in the incoming message, the monitor reports an error. This is for the receiving only option. The search is case sensitive.</p> <p><b>Example:</b> Subject:MySubject</p> <p>HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for (for example, &lt; B&gt; Hello&lt; /B&gt; World). This works for XML pages as well.</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p><b>Example:</b> /href=Doc\d+\\.html/ or /href=doc\d+\\.html/i</p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a regular expression.</p> <p><b>Example:</b> /Temperature: (d+)/</p> <p>This would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</p>
<p><b>Attachment</b></p>	<p>Enter the full path of a file to add as an attachment to the email message. Use this option to check that your email server can accept and forward messages with attached files. Optionally, you can use a regular expression to insert date and time variables to create a filename or file path.</p> <p><b>Example:</b> s/C:\firstdir\$shortYear\$\$0month\$\$0day\$/</p>
<p><b>Attachment encoding</b></p>	<p>If the attachment file content uses an encoding that is different than the encoding used on server where SiteScope is running, enter the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the attachment file.</p> <p><b>Default value:</b> windows-1252</p>

GUI Element	Description
<b>Timeout (seconds)</b>	<p>The number of seconds that the Mail monitor should wait for a mail message to be received before timing-out. Once this time period passes, the Mail monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 300 seconds</p>
<b>POP check delay (seconds)</b>	<p>After SiteScope sends the test message, it immediately logs into the mail account to verify that the message has been received. If the message has not been received, SiteScope automatically waits 10 seconds before it checks again. You can adjust this wait time by indicating an alternate number of seconds to wait in this box.</p> <p><b>Default value:</b> 10 seconds</p>
<b>SMTP user</b>	<p>Enter the user name required for SMTP authentication if the SMTP server requires authentication before sending messages.</p>
<b>SMTP password</b>	<p>Enter the password for the SMTP authentication (if required).</p>
<b>NTLM authentication</b>	<p>If NTLM authentication is used by the email server, choose if you need version 1 or version 2.</p> <p><b>Default value:</b> none</p>

# 43

---

## MAPI Monitor

This chapter includes the main concepts, tasks, and reference information for the MAPI monitor.

**This chapter includes:**

**Concepts**

- ▶ MAPI Monitor Overview on page 614

**Tasks**

- ▶ Prepare the System for Using the MAPI Monitor on page 616

**Reference**

- ▶ MAPI Monitor Settings on page 620

## MAPI Monitor Overview

The MAPI monitor checks a Messaging Application Program Interface (MAPI) server to confirm that email operations can be run. The monitor is designed to test the operation of a Microsoft Exchange Server 2003/2007. It verifies that the server is accepting requests, and also verifies that a message can be sent and retrieved. It does this by sending a standard email and deleting the mail if the message is successfully sent and received. If the received part of the monitoring fails (for example, because of a delay in sending the email or due to a short timeout for receiving the mail) the test mail remains in the mailbox. The error and warning thresholds for the monitor are set based on the email delivery time. Create a separate MAPI monitor instance for each Microsoft Exchange server in your environment.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only.

---

This section also includes:

- ▶ “Setup Requirements” on page 615
- ▶ “Configuring the Monitor” on page 615

## Setup Requirements

There are several important configuration requirements that must be performed or verified before the MAPI monitor can be used. For a description of the steps you use to configure your environment for this monitor, see “Prepare the System for Using the MAPI Monitor” on page 616. The following are several definitions that are used in the steps listed below.

- ▶ **Local Administrator.** An account that has administrative privileges on the local machine. An account can have this privilege either implicitly by having Domain Admin privileges or explicitly by adding as a member of the Administrators group on the local machine. Consult your system administrator, if necessary, for help with creating accounts.
- ▶ **MailBox Owner.** This is an "owner" account for which an Exchange mailbox has been set up. To use the MAPI monitor, this account must be a Local Administrator (see definition above) on the SiteScope server.
- ▶ **SiteScope User.** This is the account that is used to run the SiteScope service. This account must also be a Local Administrator (see definition above).

## Configuring the Monitor

For details on the monitor user interface, see “MAPI Monitor Settings” on page 620.

## Prepare the System for Using the MAPI Monitor

This task describes the steps involved in preparing the monitoring environment.

---

**Note:** For definitions of the terms Local Administrator, MailBox Owner, and SiteScope User that are used in the steps that follow, see “Setup Requirements” on page 615.

---

This task includes the following steps:

- ▶ “Create Mailbox Accounts on Each Exchange Server to be Monitored with the MAPI Monitor” on page 617
- ▶ “Add Each Exchange Mailbox Owner to the Administrators Users Group on the SiteScope Server” on page 617
- ▶ “Install Microsoft Outlook or an Equivalent MAPI 1.0 Mail Client on the SiteScope Server” on page 617
- ▶ “Configure Outlook for the MailBox User” on page 618
- ▶ “Verify the SiteScope User Logon is a Member of Administrators Group or a Domain Administrator Account” on page 618
- ▶ “Add the SiteScope User Account to the "Act as part of the operating system" Local Security Policy” on page 619
- ▶ “Configure the Monitor Properties” on page 619



## 1 Create Mailbox Accounts on Each Exchange Server to be Monitored with the MAPI Monitor

Exchange mailbox accounts are used by SiteScope to measure the roundtrip time for a message to originate and arrive in a mailbox account. The MAPI Monitor Settings pane supports up to two mailboxes per Exchange Server. If only one mailbox is specified in the MAPI Monitor Settings the same mailbox can be used for the sender and receiver accounts.

Consult your Exchange system administrator for help setting up mailbox accounts for use with the SiteScope MAPI monitor.

## 2 Add Each Exchange Mailbox Owner to the Administrators Users Group on the SiteScope Server

The Mailbox Owner accounts setup in the previous step, which are by definition domain logons, must be added to the Administrators group on the SiteScope server.

- a** Click **Start > Settings > Control Panel > Users and Passwords > Advanced tab** or open the Computer Management utility and expand the **Local Users and Groups** folder in the left pane and click the **Groups** folder.
- b** Double-click the Administrators group icon to open the Administrators Properties window.
- c** Click the **Add** button to add each Mailbox Owner you expect to use with the MAPI monitor.

---

**Note:** Make sure that the domain logon description is of the form domain\logon.

---

## 3 Install Microsoft Outlook or an Equivalent MAPI 1.0 Mail Client on the SiteScope Server

The SiteScope server requires a MAPI 1.0 client such as Outlook XP or Outlook 2003 or later. Consult your system administrator, if necessary, for help installing a compliant MAPI client.

#### 4 Configure Outlook for the MailBox User

After logging on to the SiteScope server as the MailBox User created in the first step, the Outlook wizard may start setting up an Outlook profile for the mail box. If an Outlook client is already installed, you can use that Outlook client and click **Tools > E-mail Accounts** to create a profile for the mailbox/logon you intend to use with the MAPI monitor. See your Exchange System administrator for help configuring an Outlook client on your SiteScope server.

Creating an Outlook profile is not necessary, although it may be helpful for the purpose of troubleshooting. After the wizard prompts you to set up a profile you can cancel to exit the wizard.

#### 5 Verify the SiteScope User Logon is a Member of Administrators Group or a Domain Administrator Account

The SiteScope user account must be a Local Administrator or a member of the domain admins group. To change the logon account for the SiteScope user:

- a** Open the **Services** control utility on the SiteScope server.
- b** Right-click the **SiteScope** service entry and click **Properties**. The SiteScope Properties settings page opens.
- c** Click the **Log On** tab.
- d** Verify that the SiteScope user is run as a member of Administrators group or a domain logon account. To change the logon properties, click the **This account** radio button and enter the SiteScope user logon.
- e** Restart the SiteScope server after making changes to the SiteScope service logon account.

## 6 Add the SiteScope User Account to the "Act as part of the operating system" Local Security Policy

To add the SiteScope user account to the "Act as part of the operating system" local security policy.

- a** Click **Start > Programs > Administrative Tools > Local Security Policy**. The Local Security Policy panel opens.
- b** Click the **Local Policies** folder in the left pane and then click the **User Rights Assignments** folder to display the list of policies.
- c** Double-click the **Act as part of the operating system** policy item in the right pane. The Local Security Policy Setting list opens.
- d** If the SiteScope user is not in the list of logons for this security policy setting then it must be added now. Click the **Add** button to bring up the Select Users or Groups window.
- e** Enter the SiteScope user logon using the **domain\logon** format if the SiteScope user is a domain account.
- f** After adding the SiteScope service logon, you must reload the security settings. To do this, right-click the **Security Settings** root folder in the left pane and click **Reload**.
- g** Restart the SiteScope service after making changes to security policy.

## 7 Configure the Monitor Properties

Complete the MAPI monitor configuration. For details on the monitor settings, see "MAPI Monitor Settings" on page 620.

 **MAPI Monitor Settings**

<b>Description</b>	<p>Use the MAPI monitor to monitor the availability of Microsoft Exchange 2003 and 2007. The monitor checks for email delivery time. This enables you to verify availability of the MAPI server by sending and receiving a test message in a Microsoft Exchange email account.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>➤ “Prepare the System for Using the MAPI Monitor” on page 616</li> <li>➤ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “MAPI Monitor Overview” on page 614</li> <li>➤ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## MAPI Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Receiver server</b>	Enter the host name or address of a Microsoft Exchange Server. The name can be an IP address or other name that can be resolved by the DNS server. We recommend that you copy the server name as it appears in the Properties of the email account you are using with this monitor.
<b>Receiver mailbox</b>	Enter the name (alias) of the mailbox to be used for this monitor. This is often the email account name but it may be a different name. We recommend that you copy the mailbox name as it appears in the E-Mail Account properties for the email account you are using with this monitor.
<b>Receiver domain</b>	Enter the domain to which both the owner of the mailbox being used and the Microsoft Exchange server belong.  <b>Note:</b> The owner of the mailbox to be used by this monitor must also have administrative account privileges on the machine where SiteScope is running. SiteScope also needs user account access to the domain where the Microsoft Exchange server is running.
<b>Receiver user name</b>	Enter the NT account login name for the user associated with the above email account.
<b>Receiver password</b>	Enter the NT account login password for the user name above.
<b>Sender server</b>	Enter the sender's Microsoft Exchange server name.  <b>Note:</b> <ul style="list-style-type: none"> <li>▶ The MAPI sender is ignored if an SMTP sender is specified in the <b>Sender</b> box below.</li> <li>▶ If any of the SMTP sender values are not specified, the receiver values are used instead.</li> </ul>

GUI Element	Description
<b>Sender mailbox</b>	Enter the alias of the sending mailbox.
<b>Sender domain</b>	Enter the domain to which both the sending mailbox owner and the sending Microsoft Exchange server belong.
<b>Sender user name</b>	Enter the login name for the NT account of the sending mailbox owner.
<b>Sender password</b>	Enter the NT account login password for the sender account above.
<b>Transaction timeout (seconds)</b>	Enter the number of seconds for the monitor to wait for the message to arrive before the monitor should timeout. The monitor reports an error if timeout value is met before the email message is delivered.  <b>Default value:</b> 25 seconds
<b>SMTP server</b>	Enter the SMTP server through which an outgoing message is sent.  <b>Note:</b> If you set any of the SMTP values ( <b>SMTP server</b> , <b>Sender</b> or <b>Receiver</b> ) they override the MAPI sender options.
<b>Sender</b>	Enter the email address of the SMTP sender.
<b>Receiver</b>	Enter the email address of the receiver. This must match the <b>Receiver mailbox</b> alias specified above.
<b>Attachment</b>	Enter the full path of a file to attach to the outgoing SMTP message.

# 44

---

## Memory Monitor

This chapter includes the main concepts and reference information for the Memory monitor.

### **This chapter includes:**

#### Concepts

- ▶ Memory Monitor Overview on page 623

#### Reference

- ▶ Memory Monitor Settings on page 626

### **Memory Monitor Overview**

Memory is one of the primary factors that can affect your server's performance. Use the Memory monitor to monitor how much virtual memory is currently in use on a server. Use the Pages per Second, Percentage of Virtual Memory Used, and Value of Free Memory measurements to help detect problems in this area. Each time the Memory monitor runs, it collects the measurements and displays the status in the Dashboard.

In most environments, the Memory monitor does not put a heavy load on your server. For monitoring remote UNIX servers, SiteScope needs to open the connection, while getting the data from the remote server. While the monitor actions generally do not load the either server, managing a large number of remote connections can results in some performance problems. You can use the error and warning thresholds to have SiteScope notify you if memory on a remote server starts to get low.

This section also includes:

- “Troubleshooting and Limitations” on page 624
- “Configuring the Monitor” on page 625

## **Troubleshooting and Limitations**

This section contains the following problems and solutions for the Memory monitor:

### **Pages Per Second is Affecting System Performance**

**Problem:** The number of Pages per second is consistently high (>10 pages/sec) and is affecting system performance. Pages per second measures the number of virtual memory pages that are moved between main memory and disk storage.

**Solution 1:** Add more memory.

**Solution 2:** Turn off non-critical services that are using memory, or move these services to a different machine. The SiteScope Service monitor measures the memory usage for each service.

### **Percentage of Virtual Memory Used Reaches 100%**

**Problem:** The number of Percentage of Virtual Memory Used reaches 100%, and services that are running may fail and new ones are unable to start. Percentage of Virtual Memory Used measures the percentage of memory and paging file space used.

**Solution 1:** Increase the size of the paging file. This may solve the immediate problem but may decrease performance by increasing paging. A slow increase in Virtual Memory Used is often caused by a memory leak in a service. Use the **Processes Tool** to view the memory used by each service. For details on using the tool, see “Processes Tool” on page 228.



**Solution 2:** An interim solution is to use the Service monitor to measure the service size and run a SiteScope Script Alert to restart the service when it becomes too large. If restarting the service does not fix the leak, it may be necessary to add a Script Alert to restart the server when memory usage is too high. For details on using a Script Alert, see “Working with Script Alerts” on page 1977. For details on using the Service monitor, see “Service Monitor Overview” on page 848.

**Solution 3:** Install an upgraded version of the service without the leak.

---

**Note:** When deploying the Memory monitor on a remote UNIX machine, the monitor displays swap memory usage and not virtual memory usage. To monitor virtual memory usage, deploy the UNIX Resources monitor. For details, see “UNIX Resources Monitor Overview” on page 935.

---

## Configuring the Monitor

For details on configuring the monitor, see “Memory Monitor Settings” on page 626.

 **Memory Monitor Settings**

<b>Description</b>	<p>The Memory monitor provides a tool for you to track how much virtual memory is currently in use on a server. Running out of memory can cause server applications to fail and excessive paging can have a drastic effect on performance.</p> <p>Use this page to add a monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>▶ The <b>Performance Counters Tool</b> is available when configuring this monitor to check performance counters on a specific machine in a Windows network (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Performance Counters Tool” on page 223.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Memory Monitor Overview” on page 623</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Memory Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the memory you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>

# 45

---

## Microsoft ASP Server Monitor

This chapter includes the main concepts and reference information for the Microsoft ASP Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft ASP Server Monitor Overview on page 629

#### Reference

- ▶ Microsoft ASP Server Monitor Settings on page 631

### **Microsoft ASP Server Monitor Overview**

Use the Microsoft ASP Server monitor to monitor Active Server Pages (ASP) performance parameters on Microsoft Windows NT Terminal Server 4.0 and Microsoft Windows 2000 Server. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each ASP Server you are running.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only.

---

This section also includes:

- “Setup Requirements” on page 630
- “Configuring the Monitor” on page 630

### **Setup Requirements**

- The Remote Registry service must be running on the machine where the ASP server is running if the ASP Server is running on Windows 2000.
- The Microsoft ASP Server monitor makes use of performance counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you must define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

### **Configuring the Monitor**

For details on configuring the monitor, see “Microsoft ASP Server Monitor Settings” on page 631.



## Microsoft ASP Server Monitor Settings

<b>Description</b>	<p>Monitor the availability of a Microsoft ASP server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more ASP server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<p>"Deploy a Monitor – Workflow" on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ "Microsoft ASP Server Monitor Overview" on page 629</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 354.</li> </ul>

## Microsoft ASP Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the Microsoft ASP Server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>



GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>
<b>Counters</b>	<p>The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p><b>Note when working in template mode:</b> To update counters in template browsable monitors that need a target server, click the <b>Select measurement from</b> button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the <b>Server</b> field.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p>



# 46

---

## Microsoft Exchange 5.5 Message Traffic Monitor

This chapter includes the main concepts and reference information for the Microsoft Exchange 5.5 Message Traffic monitor.

**This chapter includes:**

**Concepts**

- ▶ Microsoft Exchange 5.5 Message Traffic Monitor Overview on page 636

**Reference**

- ▶ Microsoft Exchange 5.5 Message Traffic Monitor Settings on page 637

## Microsoft Exchange 5.5 Message Traffic Monitor Overview

Use the Microsoft Exchange 5.5 Message Traffic monitor to display important statistics about messages handled by a Microsoft Exchange 5.5 server, such as a count of messages sent that are larger than a certain size, or sent to a large number of recipients.

---

**Note:**

- ▶ The Microsoft Exchange 5.5 Message Traffic monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. For details on using the template, see “Microsoft Exchange Solution Templates” on page 1725.

---

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only.

For details on configuring the monitor, see “Microsoft Exchange 5.5 Message Traffic Monitor Settings” on page 637.

## Microsoft Exchange 5.5 Message Traffic Monitor Settings

<p><b>Description</b></p>	<p>The Microsoft Exchange 5.5 Message Traffic monitor monitors message statistics of Microsoft Exchange Server 5.5.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Templates</b> context. In the template tree, expand the <b>Solution Templates</b> container. Right-click <b>Microsoft Exchange 5.5</b>, and select <b>Deploy Template</b>. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information about using templates to deploy monitors, see “SiteScope Templates” on page 1557.</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Microsoft Exchange 5.5 Message Traffic Monitor Overview” on page 636</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Microsoft Exchange 5.5 Message Traffic Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Recipient limit</b>	Enter the number (N) of recipients to use when computing the number of messages sent to more than N recipients. <b>Default value:</b> 10
<b>Query interval</b>	Enter the number of minutes to look back for messages when computing statistics. This affects how long it takes to run the monitor as a large interval could result in a large number of messages to be processed. <b>Default value:</b> 1440 minutes (one day)
<b>Message size limit</b>	Enter the number (N) of bytes to use when computing the number of messages sent larger than N bytes. <b>Default value:</b> 2000
<b>Number of domains</b>	Enter the number (N) of domains to use for reporting the top N sending domains. <b>Default value:</b> 5
<b>Number of outgoing users</b>	Enter the number (N) of users to use for reporting the top N outgoing users. <b>Default value:</b> 5
<b>Log directory</b>	Enter a UNC path to the directory where message tracking logs are stored for the Exchange 5.5 server. <b>Default value:</b> \\<server name>\tracking.log.
<b>Reporting directory</b>	Enter a location for SiteScope to save the results of each execution of this monitor. <b>Default value:</b> A default location is chosen if this box is left blank.

# 47

---

## Microsoft Exchange 2003 Mailbox Monitor

This chapter includes the main concepts and reference information for the Microsoft Exchange 2003 Mailbox monitor.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft Exchange 2003 Mailbox Monitor Overview on page 640

#### Reference

- ▶ Microsoft Exchange 2003 Mailbox Monitor Settings on page 642

## Microsoft Exchange 2003 Mailbox Monitor Overview

Use the Microsoft Exchange 2003 Mailbox monitor to display important statistics about mailboxes handled by a Microsoft Exchange 2003 server, including mailboxes that are over a certain size, and mailboxes that have not been accessed in some number of days.

---

**Note:**

- ▶ The Microsoft Exchange 2003 Mailbox monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. For details on using the template, see “Microsoft Exchange Solution Templates” on page 1725.
- ▶ This monitor is supported in SiteScopes that are running on Windows versions only.
- ▶ SiteScope must be configured to log on as a user account within the domain when running as a service, and not as Local System account.

---

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only.

This section also includes:

- ▶ “Troubleshooting and Limitations” on page 641
- ▶ “Configuring the Monitor” on page 641



## Troubleshooting and Limitations

**Problem:** You encounter one of the following errors when using the Microsoft Exchange 2003 Mailbox monitor (even though the monitor is in Good status):

- 1- Query failed: Cannot send request. Driver is not ready
- 2- Query failed: Request timed out
- 3- Query failed: Could not connect to the server

**Solution 1:** Enable WMI requests on the Microsoft Exchange 2003 server by setting the Remote Enable permission in the WMI Control for a namespace. If a user tries to connect to a namespace they are not allowed access to, they receive an error.

- 1** On the target server, select **Control Panel > Administrative Tools-> Computer Management**.
- 2** Expand **Services and Applications**.
- 3** Right-click **WMI Control** and select **Properties**.
- 4** In the **Security** tab, select the namespace and click **Security**.
- 5** Locate the appropriate account and select **Remote Enable** in the **Permissions** list.

**Solution 2:** Enable WMI requests through Windows firewall.

If the target server is running Windows Firewall (also known as Internet Connection Firewall), enable it to let remote WMI requests through. On the target server, run the following command:

```
netsh firewall set service RemoteAdmin enable
```

For more details, see the Microsoft documentation (<http://msdn.microsoft.com/en-us/library/aa389286.aspx>).

## Configuring the Monitor

For details on configuring the monitor, see “Microsoft Exchange 2003 Mailbox Monitor Settings” on page 642.

## Microsoft Exchange 2003 Mailbox Monitor Settings

<p><b>Description</b></p>	<p>The Microsoft Exchange 2003 Mailbox monitor monitors mailbox statistics of Microsoft Exchange Server 2003.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Templates</b> context. In the template tree, expand the <b>Solution Templates</b> container. Right-click <b>Microsoft Exchange 2003</b>, and select <b>Deploy Template</b>. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information about using templates to deploy monitors, see "SiteScope Templates" on page 1557.</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ "Microsoft Exchange 2003 Mailbox Monitor Overview" on page 640</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 354.</li> </ul>

## Microsoft Exchange 2003 Mailbox Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	Choose the server running Microsoft Exchange Server 2003 that you want to monitor.
<b>User name</b>	Enter the user name to use when querying the server for mailbox statistics.  The statistics are gathered by using WMI (Windows Management Instrumentation). The user name entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2.  <b>Default value:</b> If this box is left blank, the user that SiteScope is running is used.
<b>Password</b>	Enter the password for the user name entered above, or blank if user name is blank.
<b>N largest mailboxes</b>	Enter the number (N) of mailboxes to display when reporting the N largest mailboxes.  <b>Default value:</b> 5
<b>Days since access</b>	Enter the number of days (N) to use when reporting the number of mailboxes that have not been accessed in N days.  <b>Default value:</b> 30
<b>Reporting directory</b>	Enter a location for SiteScope to save the results of each execution of this monitor.  A default location is chosen if this box is left blank.
<b>Timeout (seconds)</b>	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.  <b>Default value:</b> 60 seconds



# 48

---

## Microsoft Exchange 2007 Monitor

This chapter includes the main concepts, tasks, and reference information for the Microsoft Exchange 2007 monitor.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft Exchange 2007 Monitor Overview on page 645

#### Tasks

- ▶ Configure the Microsoft Exchange 2007 Monitoring Environment on page 647

#### Reference

- ▶ Microsoft Exchange 2007 Monitor Settings on page 651

### **Microsoft Exchange 2007 Monitor Overview**

Use the Microsoft Exchange 2007 monitor to display important statistics about the messaging system handled by a Microsoft Exchange Server 2007. The statistics are gathered through Exchange Management Shell, a command-line interface (built on Microsoft Windows PowerShell technology) that is used for managing and testing Microsoft Exchange Server 2007 servers and objects.

By default, the Microsoft Exchange 2007 monitor can run command-lets (cmdlets) to provide health information about MAPI logons, Mail flow, and Search. You can also retrieve health information for Outlook Web Access and Web Services by configuring a test mailbox in the Exchange Server 2007. For details, see “Configure the Microsoft Exchange 2007 Monitoring Environment” on page 647.

Create a separate Microsoft Exchange 2007 monitor instance for each Microsoft Exchange server in your environment. The Microsoft Exchange 2007 monitor is supported on Windows versions of SiteScope only.

This section also includes:

- ▶ “Setup Requirements” on page 646
- ▶ “Configuring the Monitor” on page 647

## Setup Requirements

- ▶ To configure Microsoft Exchange 2007 monitor, Exchange Management Shell must be installed on SiteScope server. Windows PowerShell 1.0 must be installed on the computer that runs the Exchange Management Shell.
- ▶ To run each cmdlet mentioned above, the following requirements must be followed:
  - ▶ Server roles that correspond to the cmdlets you want to run must be installed on the Microsoft Exchange Server 2007. When monitoring Microsoft Exchange Server 2007, the available counters are determined according to the server roles installed. For example, if the Hub Transport and Mailbox roles are installed, the Test-MailFlow cmdlet runs. The following table shows the server roles required to run the cmdlets.

Server Role	Cmdlet
Mailbox	<ul style="list-style-type: none"> <li>▶ Test-MAPIConnectivity</li> <li>▶ Test-ExchangeSearch</li> </ul>
Hub Transport, Mailbox	Test-MailFlow
Client Access	<ul style="list-style-type: none"> <li>▶ Test-OWAConnectivity</li> <li>▶ Test-WebServicesConnectivity</li> </ul>

- ▶ You must log on to the SiteScope server using a domain account that has the permissions assigned to the Exchange Server Administrators group. The account must also be a member of the local Administrators group on that computer. For details, see “Prepare the System for Using the Microsoft Exchange 2007 Monitor” on page 649.

## Configuring the Monitor

For task details, see “Configure the Microsoft Exchange 2007 Monitoring Environment” on page 647.

For user interface details, see “Microsoft Exchange 2007 Monitor Settings” on page 651.

## Configure the Microsoft Exchange 2007 Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- ▶ “Prepare the System for Using the Microsoft Exchange 2007 Monitor” on page 647
- ▶ “Configure Additional Microsoft Exchange Server Counters - Optional” on page 648
- ▶ “Configure the Monitor Properties” on page 648
- ▶ “Schedule the Monitor - Optional” on page 648

### 1 Prepare the System for Using the Microsoft Exchange 2007 Monitor

For information on the steps you use to configure your environment for this monitor, see “Prepare the System for Using the Microsoft Exchange 2007 Monitor” on page 649.

## 2 Configure Additional Microsoft Exchange Server Counters - Optional

You must configure a test mailbox in the Microsoft Exchange Server 2007 to retrieve health information for the Outlook Web Access and Web Services cmdlets.

- a To configure a test mailbox in the Microsoft Exchange Server 2007, run the script **New-TestCasConnectivityUser.ps1** in the Exchange Server to create a test mailbox. The script can be found under **<Exchange 2007 installation directory>\Scripts**.
- b After running the command, define an initial password for this account, and press ENTER to confirm the process. A new user is created with a name similar to **CAS\_<16 digits>**.

You can run the **Get-Mailbox** cmdlet to verify that the test mailbox was created. This cmdlet retrieves a list of mailboxes, which you can use to check for the new test mailbox.

- c Repeat this process for each Exchange Mailbox Server that is to be tested.

## 3 Configure the Monitor Properties

Complete the Microsoft Exchange 2007 monitor configuration. For details on the monitor settings, see “Microsoft Exchange 2007 Monitor Settings” on page 651.

## 4 Schedule the Monitor - Optional

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only. We do not recommend setting monitor run frequency to less than 10 minutes.



## Prepare the System for Using the Microsoft Exchange 2007 Monitor

There are several important configuration requirements that must be performed or verified before the Microsoft Exchange 2007 monitor can be used. This section describes the steps you use to configure your environment for this monitor. The following are several definitions that are used in the steps listed below.

- ▶ **Local Administrator.** An account that has administrative privileges on the local machine. An account can have this privilege either implicitly by having Domain Admin privileges or explicitly by adding as a member of the Administrators group on the local machine. Consult your system administrator, if necessary, for help with creating accounts.
- ▶ **MailBox Owner.** This is an "owner" account for which an Exchange mailbox has been set up. To use the Microsoft Exchange 2007 monitor, this account must be a Local Administrator (see definition above) on the SiteScope server.
- ▶ **SiteScope User.** This is the account that is used to run the SiteScope service. This account must also be a Local Administrator (see definition above).

Before creating an Microsoft Exchange 2007 monitor, perform the following setup steps:

### **1 Create mailbox accounts on each Exchange Server to be monitored with the Microsoft Exchange 2007 monitor.**

Exchange mailbox accounts are used by Microsoft Exchange 2007 monitor to measure the performance counters on the Exchange server. Consult your Exchange system administrator if you need help setting up mailbox accounts for use with the SiteScope Microsoft Exchange 2007 monitor.

### **2 Add each Exchange Mailbox Owner to the Administrators users group on the SiteScope server.**

The Mailbox Owner accounts setup in step 1, which are by definition domain logons, must be added as to the Administrators group on the SiteScope server.

- ▶ Click **Start > Settings > Control Panel > Users and Passwords > Advanced tab** or open the Computer Management utility and expand the **Local Users and Groups** folder in the left pane and click the **Groups** folder.

- ▶ Double-click the **Administrators** group icon to open the Administrators Properties window.
- ▶ Click the **Add** button to add each Mailbox Owner you expect to use with the Exchange 2007 monitor.

---

**Note:** Make sure that the domain logon description is of the form domain\logon.

---

### **3 Verify that the SiteScope user logon is a member of Administrators group or a domain administrator account.**

---

**Important:** The SiteScope user account must be a Local Administrator or a member of the domain admins group.

---

To change the logon account for the SiteScope user:

- ▶ Open the **Services** control utility on the SiteScope server.
- ▶ Right-click the **SiteScope** service entry and click **Properties**. The SiteScope Properties settings page opens.
- ▶ Click the **Log On** tab.
- ▶ Verify that the SiteScope user is run as a member of Administrators group or a domain logon account. To change the logon properties, click the **This account** radio button and enter the SiteScope user logon.
- ▶ Restart the SiteScope server after making changes to the SiteScope service logon account.



## Microsoft Exchange 2007 Monitor Settings

<b>Description</b>	<p>Monitors statistics of Microsoft Exchange Server 2007 on Windows platforms only.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ You can create or update the Microsoft Exchange 2007 monitor even if you input the incorrect <b>Exchange Domain</b> or <b>Mailbox</b>. This is because these properties are counter specific. As a result, some counter values may not be retrieved.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the Microsoft Exchange 2007 Monitoring Environment” on page 647</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Microsoft Exchange 2007 Monitor Overview” on page 645</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Microsoft Exchange 2007 Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Exchange server</b>	Enter the name of the server running Microsoft Exchange Server 2007 that you want to monitor.
<b>Exchange domain</b>	Enter the domain name and the mailbox of the server running Microsoft Exchange Server 2007 that you want to monitor.
<b>Mailbox</b>	Enter the name (alias) of the mailbox to be used for this monitor. This is often the email account name but it may be a different name. We recommend that you copy the mailbox name as it appears in the E-Mail Account properties for the email account you are using with this monitor.
<b>Exchange PS console file path</b>	Enter the full path to the Microsoft Exchange 2007 Server Management Shell console file. <b>Example:</b> C:\Program Files\Microsoft\Exchange Server\Bin\ExShell.psc
<b>Timeout (seconds)</b>	Enables you to customize the time to wait, in seconds, for getting a response. You can set the timeout to no less than 1 second and no more than 10 minutes. <b>Default value:</b> 120 seconds

GUI Element	Description
<b>Counters</b>	<p>The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Each performance counter contains information in the following categories:</p> <ul style="list-style-type: none"> <li>▶ <b>Unit\ Type.</b> The statistic's units. Some examples of possible types of units include percent, millisecond, or KB.</li> <li>▶ <b>Component.</b> Components from which the performance counter is collected.</li> <li>▶ <b>Server Role.</b> Indicates the required server role for running the cmdlet.</li> </ul>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>



# 49

---

## **Microsoft Exchange 2000/2003/2007 Message Traffic Monitor**

This chapter includes the main concepts and reference information for the Microsoft Exchange 2000/2003/2007 Message Traffic monitor.

### **This chapter includes:**

#### **Concepts**

- ▶ Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Overview on page 656

#### **Reference**

- ▶ Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Settings on page 658

## Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Overview

Use the Microsoft Exchange 2000/2003/2007 Message Traffic monitor to display important statistics about messages handled by a Microsoft Exchange 2000/2003/2007 server, such as a count of messages sent that are larger than a certain size, or sent to a large number of recipients.

---

### Note:

- ▶ The Microsoft Exchange 2000/2003/2007 Message Traffic monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. For details on using the template, see “Microsoft Exchange Solution Templates” on page 1725.
- ▶ This monitor is supported in SiteScopes that are running on Windows versions only.
- ▶ SiteScope must be configured to log on as a user account within the domain when running as a service, and not as Local System account.

---

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only.

This section also includes:

- ▶ “Troubleshooting and Limitations” on page 657
- ▶ “Configuring the Monitor” on page 657



## Troubleshooting and Limitations

**Problem:** The monitor is in Good status, but the data displays "0".

**Solution 1:** Enable WMI requests on the Microsoft Exchange server by setting the Remote Enable permission in the WMI Control for a namespace. If a user tries to connect to a namespace they are not allowed access to, they receive an error.

- 1** On the target server, select **Control Panel > Administrative Tools-> Computer Management**.
- 2** Expand **Services and Applications**.
- 3** Right-click **WMI Control** and select **Properties**.
- 4** In the **Security** tab, select the namespace and click **Security**.
- 5** Locate the appropriate account and select **Remote Enable** in the **Permissions** list.

**Solution 2:** Enable WMI requests through Windows firewall.

If the target server is running Windows Firewall (also known as Internet Connection Firewall), enable it to let remote WMI requests through. On the target server, run the following command:

```
netsh firewall set service RemoteAdmin enable
```

For more details, see the Microsoft documentation (<http://msdn.microsoft.com/en-us/library/aa389286.aspx>).

## Configuring the Monitor

For details on configuring the monitor, see “Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Settings” on page 658.

## Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Settings

<p><b>Description</b></p>	<p>Monitors message statistics of Microsoft Exchange Server 2000/2003/2007.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Templates</b> context. In the template tree, expand the <b>Solution Templates</b> container. Right-click the Microsoft Exchange solution template version that you require, and select <b>Deploy Template</b>. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ This monitor can only be added by deploying an Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information about using templates to deploy monitors, see "SiteScope Templates" on page 1557.</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ "Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Overview" on page 656</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 354.</li> </ul>

## Microsoft Exchange 2000/2003/2007 Message Traffic Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Recipient limit</b>	Enter the number (N) of recipients to use when computing the number of messages sent to more than N recipients. <b>Default value:</b> 10
<b>Query interval</b>	Enter the number of minutes to look back for messages when computing statistics. This affects how long it takes to run the monitor as a large interval could result in a large number of messages to be processed. <b>Default value:</b> 1440 minutes (one day)
<b>Message size limit</b>	Enter the number (N) of bytes to use when computing the number of messages sent larger than N bytes. <b>Default value:</b> 2000
<b>Number of domains</b>	Enter the number (N) of domains to use for reporting the top N sending domains. <b>Default value:</b> 5
<b>Number of outgoing users</b>	Enter the number (N) of users to use for reporting the top N outgoing users. <b>Default value:</b> 5

GUI Element	Description
<p><b>Log directory</b></p>	<p>The UNC path of the messaging tracking log file directory.</p> <p><b>Default value:</b></p> <ul style="list-style-type: none"> <li>➤ For 2000/2003 versions: \\&lt;server name&gt;\&lt;server name&gt;.log</li> <li>➤ For 2007 version: \\&lt;server name&gt;\MessageTracking</li> </ul>
<p><b>Reporting directory</b></p>	<p>Enter a location for SiteScope to save the results of each execution of this monitor.</p> <p><b>Default value:</b> A default location is chosen if this box is left blank.</p>

# 50

---

## Microsoft Exchange 2003 Public Folder Monitor

This chapter includes the main concepts and reference information for the Microsoft Exchange 2003 Public Folder monitor.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft Exchange 2003 Public Folder Monitor Overview on page 662

#### Reference

- ▶ Microsoft Exchange 2003 Public Folder Monitor Settings on page 663

## Microsoft Exchange 2003 Public Folder Monitor Overview

Use the Microsoft Exchange 2003 Public Folder monitor to display important statistics about public folders handled by a Microsoft Exchange 2000/2003 server, such as access times, empty folders, folder sizes, and folders not accessed within some time period.

---

### Note:

- ▶ The Microsoft Exchange 2003 Public Folder monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. For details on using the template, see “Microsoft Exchange Solution Templates” on page 1725.
- ▶ This monitor is supported in SiteScopes that are running on Windows versions only.
- ▶ SiteScope must be configured to log on as a user account within the domain when running as a service, and not as Local System account.

---

This monitor computes statistics that do not normally change very rapidly and are not critical to system availability, so it should be scheduled to run infrequently, or on demand only.

For details on configuring the monitor, see “Microsoft Exchange 2003 Public Folder Monitor Settings” on page 663.

 **Microsoft Exchange 2003 Public Folder Monitor Settings**

<b>Description</b>	<p>Monitors public folder statistics of Microsoft Exchange Server 2003.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Templates</b> context. In the template tree, expand the <b>Solution Templates</b> container. Right-click <b>Microsoft Exchange 2003</b>, and select <b>Deploy Template</b>. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ This monitor can only be added by deploying a Microsoft Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information about using templates to deploy monitors, see “SiteScope Templates” on page 1557.</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Microsoft Exchange 2003 Public Folder Monitor Overview” on page 662</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Microsoft Exchange 2003 Public Folder Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	Select the server running Microsoft Exchange Server 2003 that you want to monitor.
<b>User name</b>	<p>Enter the user name to use when querying the server for mailbox statistics.</p> <p>The statistics are gathered by using WMI (Windows Management Instrumentation), so the user name entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2.</p> <p><b>Default value:</b> If this box is left blank, the user that SiteScope is running as is used.</p>
<b>Password</b>	Enter the password for the user name entered above, or blank if user name is blank.
<b>Days since access</b>	<p>Enter the number of days (N) to use when reporting the number of public folders that have not been accessed in N days.</p> <p><b>Default value:</b> 7</p>
<b>Timeout (seconds)</b>	<p>The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 60</p>
<b>Reporting directory</b>	<p>Enter a location for SiteScope to save the results of each execution of this monitor.</p> <p><b>Default value:</b> A default location is chosen if this box is left blank.</p>



# 51

---

## Microsoft IIS Server Monitor

This chapter includes the main concepts and reference information for the Microsoft IIS Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft IIS Server Monitor Overview on page 665

#### Reference

- ▶ Microsoft IIS Server Monitor Settings on page 668

### **Microsoft IIS Server Monitor Overview**

Use the Microsoft IIS Server monitor to monitor server performance statistics from IIS servers on Windows systems. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate IIS Server monitor instance for each IIS server in your environment.

The Microsoft IIS Server monitor supports monitoring HTTP/HTTPS services on IIS 4.0 and 5.0, and HTTP/HTTPS, FTP, NNTP and MSMQ Queue on IIS 6.

**Note:**

- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of an IIS 6 server. For details, see “Microsoft IIS Solution Template” on page 1733.
  - ▶ This monitor is supported in SiteScopes that are running on Windows versions only.
- 

This section contains the following topics:

- ▶ “Setup Requirements and User Permissions” on page 666
- ▶ “Microsoft IIS Server Topology Settings” on page 667
- ▶ “Troubleshooting and Limitations” on page 667
- ▶ “Configuring the Monitor” on page 667

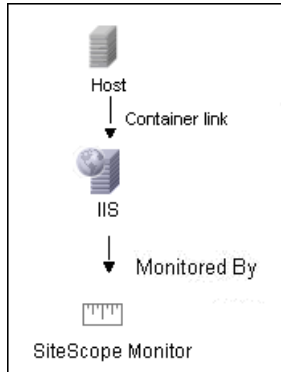
### **Setup Requirements and User Permissions**

The following are important requirements for using the Microsoft IIS Server monitor:

- ▶ The Microsoft IIS Server monitor makes use of performance counters to measure application server performance. If the servers you want to monitor require a unique login different than the account SiteScope is running under, you must define the connection to these servers in the Microsoft Windows Remote Servers container. Alternatively, you can enter the credentials of a user with administrative permissions on the server in the **Default authentication user name** and **Default authentication password** boxes in **Preferences > General Preferences**, and create the monitor without creating a Microsoft Windows Remote Server.
- ▶ The Remote Registry service must be running on the machine where the IIS server is running if IIS is running on Windows 2000.

## Microsoft IIS Server Topology Settings

The Microsoft IIS Server monitor can identify the topology of the Microsoft IIS Server being monitored. If **Include topology data when reporting to BAC** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160 in the HP Business Availability Center Documentation Library.

## Troubleshooting and Limitations

The following are guidelines for troubleshooting Microsoft IIS Server monitor problems:

- Check if the Microsoft IIS server is available and the services that should be monitored are up and running.
- If SiteScope is unable to get counters, run a test on the target remote server. If counters do not contain the required service (for example, FTP or Web Server), check if the corresponding service is running on the target machine.

## Configuring the Monitor

For details on configuring the monitor, see “Microsoft IIS Server Monitor Settings” on page 668.

 **Microsoft IIS Server Monitor Settings**

<b>Description</b>	<p>Allows you to monitor the availability and server statistics of a Microsoft IIS server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more IIS server performance counters.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<p>"Deploy a Monitor – Workflow" on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ "Microsoft IIS Server Monitor Overview" on page 665</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 354.</li> </ul>

## Microsoft IIS Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the Microsoft IIS performance statistics you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the Use already configured template remote under current template check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>
<b>Counters</b>	<p>The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p><b>Note when working in template mode:</b> To update counters in template browsable monitors that need a target server, click the <b>Select measurement from</b> button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the <b>Server</b> field.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p>

# 52

---

## Microsoft SQL Server Monitor

This chapter includes the main concepts and reference information for the Microsoft SQL Server monitor.

**This chapter includes:**

**Concepts**

- ▶ Microsoft SQL Server Monitor Overview on page 672

**Reference**

- ▶ Microsoft SQL Server Monitor Settings on page 674

## Microsoft SQL Server Monitor Overview

Use the Microsoft SQL Server monitor to monitor the server performance metrics pages for SQL Servers 6.5, 7.1, 2000, 2005, and 2008 on Windows NT systems. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Microsoft SQL Server you are running.

---

### Note:

- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of a Microsoft SQL 2005 and 2008 server. For details, see “Microsoft SQL Server 2005 Solution Template” on page 1739.
- ▶ This monitor is supported in SiteScopes that are running on Windows versions only.

---

This section contains the following topics:

- ▶ “Setup Requirements and User Permissions” on page 672
- ▶ “Microsoft SQL Server Topology Settings” on page 673
- ▶ “Configuring the Monitor” on page 673

### Setup Requirements and User Permissions

The following are requirements for using the Microsoft SQL Server monitor

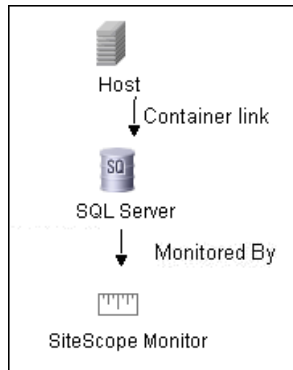
- ▶ The Microsoft SQL Server monitor uses performance counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you must define the connection to these servers in the Microsoft Windows Remote Servers container. For details, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.



- The Remote Registry service must be running on the machine where the SQL Server is running if the SQL Server is running on Windows 2000.

## Microsoft SQL Server Topology Settings

The Microsoft SQL Server monitor can identify the topology of the Microsoft SQL Servers being monitored. If **Include topology data when reporting to HP Business Availability Center** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160.

## Configuring the Monitor

For details on configuring the monitor, see “Microsoft SQL Server Monitor Settings” on page 674.

 **Microsoft SQL Server Monitor Settings**

<b>Description</b>	<p>Monitors the availability and performance of a Microsoft SQL Server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more SQL Server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Microsoft SQL Server Monitor Overview” on page 672</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Microsoft SQL Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the Microsoft SQL Server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>
<b>SQL instance name</b>	<p>Select the Microsoft SQL server instance you want to monitor from the list of SQL instances running on the selected server.</p> <p><b>Default value:</b> SQLServer (this value is displayed even if SiteScope is unable to get the instance list).</p>
<b>Counters</b>	<p>The server performance counters you want to check with this monitor. All non-default instances are dynamically loaded and displayed in the drop-down box. Use the <b>Get Counters</b> button to select counters.</p> <p><b>Note when working in template mode:</b> To update counters in template browsable monitors that need a target server, click the <b>Select measurement from</b> button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the <b>Server</b> field.</p>

GUI Element	Description
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.



# 53

---

## Microsoft Windows Dial-up Monitor

This chapter includes the main concepts and reference information for the Microsoft Windows Dial-up monitor.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft Windows Dial-up Monitor Overview on page 679

#### Reference

- ▶ Microsoft Windows Dial-up Monitor Settings on page 682

### **Microsoft Windows Dial-up Monitor Overview**

Use the Microsoft Windows Dial-up monitor to measure the availability and performance of your Internet applications from a dial-up user's perspective. The Microsoft Windows Dial-up monitor can also be used to monitor the availability and performance of remote access servers.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only.

---

If you are primarily interested in dial-up availability, then you can just have the Microsoft Windows Dial-up monitor try to connect, and if successful, run one or two low impact monitors to verify that the connection is operating properly. If you are more interested in the perspective of a dial-up user, then running a suite of monitors that represent typical user tasks gives you more complete assessment.

To set up the Remote Access Service on a Windows NT machine, go to the Network Control Panel, and add the service. At that time you also have the option of adding one or more modems as Remote Access modems. At least one of the modems has to have dial out capability for this monitor to work.

This section contains the following topics:

- "Status" on page 680
- "Scheduling the Monitor" on page 681
- "Troubleshooting and Limitations" on page 681
- "Configuring the Monitor" on page 682

## **Status**

Each time the Microsoft Windows Dial-up monitor runs, it returns a reading and status message and writes them in the monitoring log file. The reading is the current value returned by the monitor. For example, "5 of 5 monitors OK in 55 sec", or "The line was busy". The status is logged as either OK or warning.

For reports, the Microsoft Windows Dial-up Monitors saves the total time taken (to connect and run the monitors), the connect time (the time for the modem to establish a physical connection), the authorization time (the time after physical connection is established before the connection can actually be used), and the percentage of the monitors run that were OK.



## Scheduling the Monitor

The Microsoft Windows Dial-up monitor stops other monitors from running while it is connected, so you should take into account the number and kinds of monitors that are running while the connection is established as well as the number of other monitors that are running. If SiteScope is running only Microsoft Windows Dial-up Monitors, then you can schedule them more frequently (every 5 or 10 minutes). However, if you are monitoring many other items, choose a large interval (hours), so that other monitoring is not disrupted.

Only one Microsoft Windows Dial-up monitor can run at a time, so if you have more than one Microsoft Windows Dial-up monitor, take that into account when scheduling the monitors.

## Troubleshooting and Limitations

This section includes the following troubleshooting topics for the Microsoft Windows Dial-up monitor:

- ▶ The Microsoft Windows Dial-up monitor should not be used on a machine that is used for accessing resources outside of the local network. This is because the monitor uses Remote Access, which affects the entire machine's network connectivity when it establishes a connection. For example, if you are using a Web browser on the machine where SiteScope is running a Microsoft Windows Dial-up monitor, and the Microsoft Windows Dial-up monitor is connected, all the requests by the browser out to the Internet also use the dial-up connection. This affects the speed of the browser and the reading from the Microsoft Windows Dial-up monitor.
- ▶ The Microsoft Windows Dial-up monitor prevents the other SiteScope monitors (those not being run by this Dial-up monitor) from running while the dial-up connection is established (they are held up until the Microsoft Windows Dial-up monitor is completed).
- ▶ No two Microsoft Windows Dial-up Monitors can be run at the same time.

- The Microsoft Windows Dial-up monitor uses the dial-up connection only for requests outside of the local network. If you have monitors that access network resources on the local network, their readings are the same as if the Microsoft Windows Dial-up monitor was not used. However, monitors that access network resources outside the local network use the dial-up connection. For example, if you ran two Ping monitors in the Microsoft Windows Dial-up monitor, one of which was yourserver.com (on the local network), and the other of which was externalserver.com (on an external network), the yourserver.com Ping would be very fast, because it would use the LAN, while the externalserver.com Ping would take longer, because it would go through the dial-up connection.

### Configuring the Monitor

For details on configuring the monitor, see “Microsoft Windows Dial-up Monitor Settings” on page 682.

## Microsoft Windows Dial-up Monitor Settings

<p><b>Description</b></p>	<p>The Windows Dial-up monitor (available only on the Windows NT version of SiteScope) uses the Windows NT Remote Access Service to connect to an Internet Service Provider or Remote Access server and optionally runs a user-defined set of monitors. The monitor confirms that the dial-up connection can be established, and measures the performance of the connection and of the network services using the dial-up connection.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<p>Monitors must be created in a group in the monitor tree.</p>

<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Microsoft Windows Dial-up Monitor Overview” on page 679</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### Microsoft Windows Dial-up Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Account Settings</b>	
<b>Phone number</b>	Enter the phone number for the dial-up account, adding any extra modem digits or pauses that are required. <b>Example:</b> 9,4432266 includes a "9," for getting an outside line. Insert a comma wherever you need a short pause.
<b>Account user name</b>	The login name for the dial-up account.
<b>Account password</b>	The password for the dial-up account.

GUI Element	Description
<b>Advanced Settings</b>	
<b>Timeout (seconds)</b>	<p>The timeout limits the total time that the Microsoft Windows Dial-up monitor takes to connect, authenticate, and run each of its monitors. If the time ever exceeds this time, then the connection is hung up, and the monitor completes with a timeout error.</p> <p><b>Default value:</b> 60 seconds</p>
<b>Monitor Settings</b>	
<b>Monitor(s) to run</b>	<p>Select the groups and/or monitors that you want to run while the dial-up connection is established.</p> <p>Monitors that are used by Microsoft Windows Dial-up Monitors should not be scheduled to run by themselves because some of their data would be through the dial-up connection, and some of their data would be through the local connection.</p> <p>Make sure that the <b>Frequency</b> box for these monitors is set to 0. For details, see “Monitor Run Settings” on page 358.</p>

# 54

---

## Microsoft Windows Event Log Monitor

This chapter includes the main concepts and reference information for the Microsoft Windows Event Log monitor.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft Windows Event Log Monitor Overview on page 685

#### Reference

- ▶ Microsoft Windows Event Log Monitor Settings on page 687

### **Microsoft Windows Event Log Monitor Overview**

Use the Microsoft Windows Event Log monitor to monitor added entries in one of the Microsoft Windows Event Logs (System, Application, or Security). The Microsoft Windows Event Log monitor examines log entries made only after the time that the monitor is created. Each time the monitor runs thereafter, it examines only those entries added since the last time it ran. You can choose to filter out messages that are not important by using the boxes listed under Monitor Settings to specify values that must appear in the event entry for the entry to match.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only.

---

This section contains the following topics:

- “Configuring SiteScope Alerts” on page 686
- “Status” on page 686
- “Configuring the Monitor” on page 686

## Configuring SiteScope Alerts

When setting up SiteScope alerts for Microsoft Windows Event Log Monitors that are set to alert **For each event matched**, it is most useful to select the NTEventLog template for the E-mail, Pager, SNMP, or Script alert. This alert template sends the alert with the event entry fields broken out. The type of SiteScope alert triggered depends on the type of the log event entry:

Event Log Entry Type	SiteScope Alert Type
Error	Error
Warning	Warning
Information	OK

Each time the Microsoft Windows Event Log monitor runs, it returns a reading and status message and writes them in the `<SiteScope root directory>\logs\SiteScopeyyyy_mm_dd.log` file.

## Status

The status for the Microsoft Windows Event Log monitor includes the number of entries examined, and the number of entries matched. If an interval is specified, the number of events in that interval is also displayed. Matched entries and interval entries can trigger alerts.

## Configuring the Monitor

For details on configuring the monitor, see “Microsoft Windows Event Log Monitor Settings” on page 687.

## Microsoft Windows Event Log Monitor Settings

<p><b>Description</b></p>	<p>The Microsoft Windows Event Log monitor is used to monitor one of the Microsoft Windows Event Logs (System, Application, or Security) for added entries.</p> <p>This monitor is available only on the Windows version of SiteScope.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>▶ The <b>Event Log Tool</b> is available when configuring this monitor to display portions of the Windows Event Log (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Event Log Tool” on page 205.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Microsoft Windows Event Log Monitor Overview” on page 685</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Microsoft Windows Event Log Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the event log you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>



GUI Element	Description
<b>Log name</b>	<p>The event log to monitor. Select from the following logs:</p> <ul style="list-style-type: none"> <li>▶ Application</li> <li>▶ Directory Service</li> <li>▶ DNS</li> <li>▶ File Replication Service</li> <li>▶ Security</li> <li>▶ System</li> </ul> <p><b>Note:</b> This is a static list of those logs available when deploying this monitor. These log files do not necessarily exist on the server you are monitoring.</p>
<b>Event type</b>	<p>The event types to match. Select from the following event types:</p> <ul style="list-style-type: none"> <li>▶ Any</li> <li>▶ Error</li> <li>▶ Warning</li> <li>▶ Error or warning</li> <li>▶ Information</li> </ul>
<b>Run alerts</b>	<p>Select the method for running alerts.</p> <ul style="list-style-type: none"> <li>▶ If <b>For each event matched</b> is chosen, then the monitor triggers alerts for every matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error).</li> <li>▶ If <b>Once, after all events have been checked</b> is chosen, then the monitor counts up the number of matches and triggers alerts based on the warning and error threshold settings.</li> </ul>

GUI Element	Description
<p><b>Source and ID match</b></p>	<p>Enter the match string identifying the source of the event and the event ID in the form: &lt;Event Source&gt;:&lt;Event ID&gt;.</p> <p><b>Example:</b> Print:20 matches event source named Print and event ID of 20.</p> <p>To match against all events from a specific source, enter just the event source name.</p> <p><b>Example:</b> W3SVC</p> <p>To match an exact event ID from an event source, specify both.</p> <p><b>Example:</b> Service Control Mar:7000</p> <p><b>Note:</b> You can click the <b>Open Tool</b> button to use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</p>

GUI Element	Description
<p><b>Source and ID do not match</b></p>	<p>Enter the string identifying the source of the event and the event ID to NOT MATCH in the form: &lt;Event Source&gt;:&lt;Event ID&gt;.</p> <p><b>Example:</b> Print:20 means event source named Print and event ID of 20 must not be in the event in order to have a match.</p> <p>To not match all events from a particular source, specify just the source name.</p> <p><b>Example:</b> W3SVC</p> <p>To not match an exact event ID from an event source, specify both.</p> <p><b>Example:</b> Service Control Mar:7000</p> <p>You can also use a regular expression for a more complex NOT MATCH.</p> <p><b>Example:</b></p> <ul style="list-style-type: none"> <li>▶ to not match all Perflib sources from 200 to 299 use: /Perflib:2\d\d/</li> <li>▶ to not match all events from the Perflib source, use: Perflib:*</li> </ul> <p><b>Note:</b> You can click the <b>Open Tool</b> button to use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</p>
<p><b>Description match</b></p>	<p>Enter the text string to match against the description text for the event entry. Thresholds that are defined as value/value 2/value3/value4 refer to the matches found in the event description.</p> <p>The description text is the same as the description that is displayed when viewing the detail of an event log entry in the Windows Event Viewer.</p> <p><b>Note:</b> You can click the <b>Open Tool</b> button to use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</p>

GUI Element	Description
<p><b>Description does not match</b></p>	<p>Enter the text string description that must not be in the event in order to have a match.</p> <p>The description text can be viewed in the detail view of the event log entry by using the Windows Event Viewer.</p> <p><b>Note:</b> You can click the <b>Open Tool</b> button to use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</p>
<p><b>Event category</b></p>	<p>Match the category number of the event entry. Leaving this blank matches events with any category.</p>
<p><b>Event machine</b></p>	<p>Match against the machine that added the entry to the log file. Leaving this blank matches events with any machine.</p>
<p><b>Interval (minutes)</b></p>	<p>Enter a time period for which matching event log entries are totaled. This is useful when the case you are interested in is a quantity of events happening in a given time period.</p> <p><b>Example:</b> If you wanted to detect a succession of service failures, 3 in the last 5 minutes, you would specify 5 minutes for the interval, and then change the <b>Error If</b> threshold to <b>matches in interval &gt;= 3</b>.</p> <p><b>Note:</b> This field is not available when <b>For each event matched</b> is selected in the <b>Run alert</b> field.</p>

# 55

---

## Microsoft Windows Media Player Monitor

This chapter includes the main concepts and reference information for the Microsoft Windows Media Player monitor.

**This chapter includes:**

**Concepts**

- ▶ Microsoft Windows Media Player Monitor Overview on page 694

**Reference**

- ▶ Microsoft Windows Media Player Monitor Settings on page 695

## Microsoft Windows Media Player Monitor Overview

Use the Microsoft Windows Media Player monitor to monitor availability and delivery quality parameters for media files and streaming data compatible with Windows Media Servers. This monitor supports monitoring Windows Media Player 7.x, 9.x, 10.x, and 11.0. You can monitor multiple parameters or counters with a single monitor instance. This enables you to report on delivery performance. Create a separate monitor instance for files or data streams that are representative of the content available from the site you want to monitor.

---

**Note:**

- ▶ This monitor is supported in SiteScopes that are running on Windows versions only.
- ▶ You should monitor only video streams, not audio streams, with this monitor.

---

You must have an instance of Windows Media Player installed on the machine where SiteScope is running to use this monitor.

For a list of the Media Player performance parameters or counters you can check with the Microsoft Windows Media Player monitor, see “Performance Counters” on page 697.

For details on configuring the monitor, see “Microsoft Windows Media Player Monitor Settings” on page 695.



## Microsoft Windows Media Player Monitor Settings

<b>Description</b>	<p>The Microsoft Windows Media Player monitor enables you to emulate a user playing media or streaming data from a Windows Media Server. The error and warning thresholds for the monitor can be set on one or more Windows Media Player performance statistics.</p> <p>This monitor does not support the .asx or .mov formats. Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>Microsoft Windows Media Player Tool</b> is available when configuring this monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Microsoft Windows Media Player Tool” on page 218.</li> </ul>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Microsoft Windows Media Player Monitor Overview” on page 694</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Microsoft Windows Media Player Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>URL</b>	<p>Enter the URL of the media file or streaming source you want to monitor. This should be the URL of the media file.</p> <p><b>Example:</b> mms://&lt;servername&gt;/sample.asf for a unicast stream or http://&lt;servername&gt;/stationid.nsc for a multicast stream using a Windows Media Server multicast station program.</p> <p><b>Note:</b> This monitor does not support the .asx or .mov formats.</p>
<b>Duration (milliseconds)</b>	<p>Enter the playback duration that the monitor should use for the media file or streaming source. The duration value does not need to match the duration of the media contained in the file.</p> <p>If the media content of the file or source you are monitoring is less than the duration value selected for the monitor, the monitor plays the entire media content and reports the results, including the time required to play the media content.</p> <p><b>Default value:</b> 15000 milliseconds</p>
<b>Counters</b>	<p>Select the media player performance parameters or counters you want to check with the Microsoft Windows Media Player monitor.</p> <p>For details on the available parameters or counters, see “Performance Counters” on page 697.</p>



## Performance Counters

The media player performance parameters or counters you can check with the Microsoft Windows Media Player monitor include:

GUI Element	Description
<b>Buffering count</b>	The number of times the Player had to buffer incoming media data due to insufficient media content.
<b>Buffering time</b>	The time spent waiting for sufficient media data to continue playing the media clip.
<b>Interrupts</b>	The number of interruptions encountered while playing a media clip. This includes buffering and playback errors.
<b>Packets lost</b>	The number of lost packets not recovered (applicable to network playback).
<b>Packets recovered</b>	The number of lost packets successfully recovered (applicable to network playback).
<b>Packet quality</b>	The percentage ratio of packets received to total packets.
<b>Ratio bandwidth</b>	The ratio (as a percentage) of the actual bandwidth used to the recommended bandwidth.  <b>Example:</b> If the recommended bandwidth is 100 bps and the actual bandwidth is 50 bps, the ratio bandwidth is 50%. If the recommended bandwidth is 50 bps and the actual bandwidth is 100 bps, the ratio bandwidth is 200%.
<b>Recommended bandwidth</b>	The recommended bandwidth in bits per second. When a .wmv file is opened in Media Player, the property <b>bitrate</b> is the recommended bandwidth. This bandwidth is embedded in the stream itself.
<b>Recommended duration</b>	The total duration of the media clip in seconds. This value is not effected by what was already played.
<b>Sampling rate</b>	The sampling rate in milliseconds, for collecting statistics.
<b>Stream count</b>	The packet count.

GUI Element	Description
<b>Stream max</b>	The maximum number of packets.
<b>Stream min</b>	The minimum number of packets.
<b>Stream rate</b>	The packet rate indicating the speed at which the clip is played: 1 is the actual speed, 2 is twice the original speed, and so on.
<b>Time quality</b>	The percentage of stream samples received on time (no delays in reception).

# 56

---

## Microsoft Windows Media Server Monitor

This chapter includes the main concepts and reference information for the Microsoft Windows Media Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft Windows Media Server Monitor Overview on page 699

#### Reference

- ▶ Microsoft Windows Media Server Monitor Settings on page 701

### **Microsoft Windows Media Server Monitor Overview**

Use the Microsoft Windows Media Server monitor to monitor the server performance parameters for Microsoft Windows Media Servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning.

Create a separate monitor instance for each Windows Media Server you are running. This monitor supports all versions of Microsoft Windows Media Server via perfmon.

**Note:**

- This monitor is supported in SiteScopes that are running on Windows versions only.
  - By default, SiteScope monitors the Microsoft Windows Media Server default services, **Windows Media Station Service** and **Windows Media Unicast Service**. To monitor other services, add the service names (separated by commas) to the **Microsoft Windows Media Server monitor service names** box in **Preferences > Infrastructure Preferences > Monitor Settings**.
- 

This section also includes:

- “Setup Requirements and User Permissions” on page 700
- “Configuring the Monitor” on page 700

## **Setup Requirements and User Permissions**

The Microsoft Windows Media Server monitor uses performance counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you must define the connection to these servers under the Microsoft Windows Remote Servers container in the remote server tree. For details, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.

## **Configuring the Monitor**

For details on configuring the monitor, see “Microsoft Windows Media Server Monitor Settings” on page 701.

## Microsoft Windows Media Server Monitor Settings

<b>Description</b>	<p>The Microsoft Windows Media Server monitor enables you to monitor the availability of a Microsoft Windows Media server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more Windows Media server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Microsoft Windows Media Server Monitor Overview” on page 699</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Microsoft Windows Media Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<p><b>Server</b></p>	<p>The server where the Windows Media Server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>
<b>Counters</b>	<p>The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p><b>Note when working in template mode:</b> To update counters in template browsable monitors that need a target server, click the <b>Select measurement from</b> button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the <b>Server</b> field.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p>





# 57

---

## Microsoft Windows Performance Counter Monitor

This chapter includes the main concepts and reference information for the Microsoft Windows Performance Counter monitor.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft Windows Performance Counter Monitor Overview on page 706

#### Reference

- ▶ Microsoft Windows Performance Counter Monitor Settings on page 707

## Microsoft Windows Performance Counter Monitor Overview

Use the Microsoft Windows Performance Counter monitor to monitor the values of any Windows performance statistic running on Windows XP Pro, Windows NT Server 4.0, and Windows Server 2000/2003/2008. Each time the Microsoft Windows Performance Counter monitor runs, it returns a reading and a status message and writes them in the monitoring log file. The status is displayed in the group details table for the monitor which represents the current value returned by this monitor. The status is logged as either good, warning, or error. An error occurs if the counter could not be read, or if measurements are within the error threshold range.

---

**Note:** This monitor is also supported in SiteScopes that are running on UNIX versions if:

- ▶ **Allow Unix to NT** is selected in **Preferences > Infrastructure Preferences > General Settings**.
- ▶ The remote server used for monitoring has been configured for SSH. For details, see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1317.

---

For details on configuring the monitor, see “Microsoft Windows Performance Counter Monitor Settings” on page 707.

## Microsoft Windows Performance Counter Monitor Settings

<p><b>Description</b></p>	<p>The Microsoft Windows Performance Counter monitor tracks the values of any Windows performance statistic. These are the same statistics that can be viewed using the Microsoft Management Console under Windows.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>➤ Monitors must be created in a group in the monitor tree.</li> <li>➤ This monitor is also supported in SiteScopes that are running on UNIX versions if:             <ul style="list-style-type: none"> <li>➤ <b>Allow Unix to NT</b> is selected in <b>Preferences &gt; Infrastructure Preferences &gt; General Settings</b>.</li> <li>➤ The remote server used for monitoring has been configured for SSH.</li> </ul> </li> <li>➤ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>➤ The <b>Performance Counters Tool</b> is available when configuring this monitor to check performance counters on a specific machine in a Windows network (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see "Performance Counters Tool" on page 223.</li> </ul>

<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"><li>▶ “Microsoft Windows Performance Counter Monitor Overview” on page 706</li><li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li></ul>

## Windows Performance Counter Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<p><b>Server</b></p>	<p>The server on which you want to monitor Windows performance statistics. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p>When using a settings file from the Microsoft Windows Performance Counter monitor, all counters are measured on the server specified by this entry.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<p><b>Browse Servers</b></p>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>

GUI Element	Description
<b>Add Remote Server</b>	Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.
<b>PerfMon chart file</b>	<p>Select the Microsoft Windows Performance Counter monitor setting file you want to use for your settings. These files can be saved in the Microsoft Management Console (perfmon) and have either a .pmc or .pmw extension. On Windows 2000 Platform these can be saved using the .htm format. The files in this list all reside in the &lt;SiteScope root directory&gt;\<b>templates.perfmon</b> directory. There are a number of default files in the standard SiteScope distribution.</p> <p><b>Note:</b> If you make your own settings file, it must be placed in the &lt;SiteScope root directory&gt;\<b>templates.perfmon</b> directory. You can optionally specify the settings directly for a single counter in the <b>Counter</b> box below.</p> <p>If you create your own .pmc file, any server specified in the .pmc file is ignored by SiteScope. The queried server is the one in the <b>Server</b> box (see above). Therefore, do not include identical counters directed at different servers in a single .pmc file. One .pmc file can be used by more than one Microsoft Management Console instance, but any single instance of the Microsoft Management Console only queries one server regardless of the servers assigned in the .pmc.</p> <p>If you have specified the settings directly in the <b>Object</b> box below, this list displays (<b>Custom object</b>).</p>
<b>Object</b>	Enter the name of the high level item that is being measured, such as Processor or Server. It is the same as the Object in the Microsoft Management Console. The object name is case sensitive. If you are using a Performance monitor file for counter settings, leave this item blank.

GUI Element	Description
<b>Counter</b>	Enter the specific aspect of the Object that is measured, such as Interrupts/sec. It is the same as the Counter in the Microsoft Windows Performance monitor application. The counter name is case sensitive. If you are using a Microsoft Windows Performance monitor file for counter settings, leave this item blank.
<b>Units</b>	Enter the units to be displayed with the counter's values to make them more readable.
<b>Instance</b>	Some counters can have multiple instances, for example, on machines with two CPUs, there are two instances of the Processor object. Enter the instance in the Microsoft Windows Performance monitor application. The instance name is case sensitive. If you are using a Microsoft Windows Performance monitor file for counter settings, leave this item blank. If you leave this blank and there are multiple instances, the first instance in the list is selected.
<b>Scale</b>	<p>If you want the raw performance counter value scaled to make it more readable, select one of the predefined choices using the <b>Commonly used values</b> list, or enter a numeric value in the <b>Other values</b> box.</p> <p>The raw value of the counter is multiplied by the scale to determine the value of the monitor. The kilobytes option divides the raw value by 1,024 (the number of bytes in 1 K), and the megabytes option divides the raw value by 1,048,576 (the number of bytes in 1 MB). If there are multiple counters specified by using a Microsoft Windows Performance monitor file, this scaling applies to all counters.</p> <p><b>Default value:</b> 1</p>





# 58

---

## Microsoft Windows Resources Monitor

This chapter includes the main concepts, tasks, and reference information for the Microsoft Windows Resources monitor.

### **This chapter includes:**

#### **Concepts**

- ▶ Microsoft Windows Resources Monitor Overview on page 714

#### **Tasks**

- ▶ Configure the Microsoft Windows Resources Monitoring Environment on page 717

#### **Reference**

- ▶ Microsoft Windows Resources Monitor Settings on page 720

## Microsoft Windows Resources Monitor Overview

Use the Microsoft Windows Resources monitor to monitor the server performance statistics from remote Windows servers running on Windows XP Pro, Windows NT Server 4.0, and Windows Server 2000, 2003, and 2008. This enables you to watch server loading for performance, availability, and capacity planning. You can monitor multiple parameters or counters on a single, remote server with each monitor instance. Create one or more Microsoft Windows Resources monitor instances for each remote server in your environment.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only.

---

This section contains the following topics:

- “Setup Requirements and User Permissions” on page 715
- “Server-Centric Report” on page 715
- “Configuring the Monitor to Run on Windows 2003 as a Non-Administrator User” on page 716
- “Troubleshooting and Limitations” on page 716
- “Configuring the Monitor” on page 716

## Setup Requirements and User Permissions

The following are important requirements for using the Microsoft Windows Resources monitor:

- ▶ The Microsoft Windows Resources monitor uses performance counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you must define the connection to these servers under the Microsoft Windows Remote Servers option in the SiteScope Preferences container. For details, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
- ▶ When monitoring Windows servers configured using SSH, you must use the **Direct registry queries** option for the **Collection method** in the Monitor Settings panel when you configure the monitor.

## Server-Centric Report

You can create a Server-Centric Report for the Windows server by clicking the server name in the Target column of the row corresponding to the Microsoft Windows Resources monitor in Dashboard. For details, see “Server-Centric Report” on page 1881.

## Configuring the Monitor to Run on Windows 2003 as a Non-Administrator User

For the Microsoft Windows Resources monitor to monitor a Windows 2003 machine if the SiteScope user account is not in the Administrators group, you must either:

- ▶ use the same domain account on both the SiteScope and the remote monitored system, or
- ▶ use local accounts on both systems, provided that the user accounts have the same name and password and are always synchronized on both systems. You cannot use **Local System** or other similar system predefined accounts that do not enable you to specify a password for them.

In addition, you must configure the user account settings on SiteScope and the remote monitored machine to log on using the selected non-administrator user account (domain or local account). You can then use a standard Windows perfmon utility to verify that it works. For details on how to perform this task, see “Configure the Microsoft Windows Resources Monitoring Environment” on page 717.

## Troubleshooting and Limitations

**Problem:** Getting invalid CPU value error message in <SiteScope root directory>\logs\RunMonitor.log file when using perfmon monitors on VMWare host servers.

**Solution:** Use the VMWare Performance monitor to measure CPU on VMWare host servers.

## Configuring the Monitor

For task details, see “Configure the Microsoft Windows Resources Monitoring Environment” on page 717.

For user interface details, see “Microsoft Windows Resources Monitor Settings” on page 720.

## **Configure the Microsoft Windows Resources Monitoring Environment**

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Configure User Account Settings on SiteScope” on page 717
- “Configure User Account Settings on the Remote Monitored Machine:” on page 717
- “Verify that the Non-Administrator User Account Works” on page 719
- “Configure the Monitor Properties” on page 719

### **1 Configure User Account Settings on SiteScope**

The user account settings on SiteScope must be configured to log on using the selected non-administrator user account.

- a** In the **Services** control panel, right-click the **SiteScope** service, and then click **Properties**. The SiteScope Properties dialog box opens.
- b** Click the **Log On** tab, and configure the user account to log on using the selected non-administrator user account (domain or local account).

### **2 Configure User Account Settings on the Remote Monitored Machine:**

The user account settings on the remote monitored server must be configured to log on using the selected non-administrator user account.

- a** Check that you can access the remote machine. Perform a ping test and check DNS resolves the server name with its IP address.

We recommend that you check there are no other network-related problems by using the selected user account to map a network drive of the monitored machine to the drive used on the SiteScope machine.

- b** In the **Services** control panel, check that the **RemoteRegistry** service is running and that the selected user account has access to it. You can use the following command from the Windows 2003 Resource Kit (run it under an administrator account):

```
subinacl /service RemoteRegistry /grant=tester=f
```

This command grants Full Access to the RemoteRegistry service for the local user tester.

- c** Add the domain or local user account to be used into the **Performance Monitor Users** and **Performance Log Users** local user groups. Make sure that these groups have at least read permissions for the following registry key (and all its subkeys):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib]
```

---

**Tip:** To check read permissions, select **Start > Run**, and type **Regedt32.exe**. In the Registry Editor, select the registry key, click **Security**, and select **Permissions**. In the Name pane, highlight the user SiteScope uses to access the remote machine, and make sure that the **Allow** check box for **Read** is selected in the **Permissions** pane.

---

- d** Make sure that the domain or local user account to be used has at least read permissions on the following objects:
- Registry key:  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg]
  - Files in %WINDIR%\System32\perf?XXX.dat, where **XXX** is the basic language ID for the system. For example, 009 is the ID for the English version.

---

**Note:** If the required Performance Counter Library Values are missing or are corrupted, follow the instructions in Microsoft knowledge base article KB300956 (<http://support.microsoft.com/kb/300956/en-us>) to manually rebuild them.

---

### 3 Verify that the Non-Administrator User Account Works

After configuring the user account settings, verify that they work.

- a** Launch a standard Windows perfmon utility. You can either:
- ▶ launch it interactively when logged on to the SiteScope machine with the selected user account by typing `perfmon`, or
  - ▶ launch it when logged on to the SiteScope machine with some other account through the `RunAs` command, which enables you to launch commands under different user account. Enter the following command:

```
runas /env /netonly /user:tester "mmc.exe perfmon.msc"
```

Then enter the password (in this example, for the `tester` account), and the command is run under the `tester` user account.

- b** After the Performance window opens, right-click in the right graph area and select **Add Counters**. The Add Counters dialog box opens.
- c** Select **Choose counters from computer** and enter the remote monitored machine name or its IP address in the box.

Press the `TAB` key. If the `perfmon` utility is able to connect to the remote machine, the Performance object box is filled in with the performance objects that can be monitored from the remote machine.

### 4 Configure the Monitor Properties

Complete the Microsoft Windows Resources monitor configuration. For details on the monitor settings, see “Microsoft Windows Resources Monitor Settings” on page 720.

## Microsoft Windows Resources Monitor Settings



<b>Description</b>	<p>The Microsoft Windows Resources monitor enables you to monitor system performance data using the Performance Data Helper (PDH) interface on Windows systems. The error and warning thresholds for the monitor can be set on one or more performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The performance parameters or counters available for the Microsoft Windows Resources monitor vary depending on what operating system options and applications are running on the remote server.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode:             <ul style="list-style-type: none"> <li>▶ You can use regular expressions to define counters.</li> <li>▶ The <b>Add Remote Server</b> button is not displayed.</li> </ul> </li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the Microsoft Windows Resources Monitoring Environment” on page 717</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Microsoft Windows Resources Monitor Overview” on page 714</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>



## Microsoft Windows Resources Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The Microsoft Windows server that you want to monitor. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Server to get measurements from</b>	<p>(Available in template mode only) Select the name of any SiteScope remote server from which you want to get counters (it must be accessible in the domain using NETBIOS).</p>

GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>
<b>Available Counters</b>	<p>Displays the available measurements for this monitor. For each measurement, select the <b>Object</b>, <b>Instances</b> and <b>Counters</b> you want to check with the Microsoft Windows Resources monitor, and click the <b>Add Selected Counters</b>  button. The selected measurements are moved to the Selected Counters list.</p>
<b>Selected Counters</b>	<p>Displays the measurements currently selected for this monitor, and the total number of selected counters. To remove measurements selected for monitoring, select the required measurements, and click the <b>Remove Selected Counters</b>  button. The measurements are moved to the Available Counters list.</p>

GUI Element	Description
<b>Collection method</b>	<p>Select the collection method from the following options:</p> <ul style="list-style-type: none"> <li>▶ <b>Microsoft Windows PDH Library.</b> This is the default and most common option.</li> <li>▶ <b>Use global setting.</b> Instructs the monitor to use the value configured in the <b>master.config</b> file for the <b>_wormCollectionMethod</b> property. If this property has not been added to the <b>master.config</b> file, the default option is used.</li> <li>▶ <b>Direct registry queries.</b> Use this option if Windows PDH library is not accessible or if the monitor is having trouble using the Windows PDH library. You must use this option when monitoring Windows servers configured using SSH.</li> </ul> <p><b>Note:</b> The collection method option is available only when the target remote server uses the NetBIOS protocol (not SSH or WMI).</p>
<b>Enable Server-Centric Report</b>	<p>Select to enable collecting data specifically for generating the Server-Centric Report. The report displays various measurements for the server being monitored. For details, see “Generating a Server-Centric Report” on page 1881.</p>



# 59

---

## Microsoft Windows Services State Monitor

This chapter includes the main concepts and reference information for the Microsoft Windows Services State monitor.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft Windows Services State Monitor Overview on page 725

#### Reference

- ▶ Microsoft Windows Services State Monitor Settings on page 727

### **Microsoft Windows Services State Monitor Overview**

Use the Microsoft Windows Services State monitor to monitor the services installed and running on remote Windows servers running on Windows XP Pro, Windows NT Server 4.0, and Windows Server 2000/2003/2008. By default, the monitor returns a list of all of the services that are set to be run automatically on the remote server. You can filter the list of services returned by the monitor using regular expressions. The monitor displays the number of services running and related statistics along with a summary listing of the services installed on the remote server.

**Note:**

- ▶ This monitor is supported in SiteScopes that are running on Windows versions only.
  - ▶ The Microsoft Windows Services State monitor only retrieves a list of installed services. It does not query the list of processes that may be running on the remote machine (use the Service monitor for this).
- 

This section also includes:

- ▶ “Configuring Alerts” on page 726
- ▶ “Configuring the Monitor” on page 726

### **Configuring Alerts**

To use this monitor to create event alerts, configure alert definitions associated with this monitor to alert **Once, after the condition has occurred exactly 1 times**. This is because the Microsoft Windows Services State monitor only signals a change in state for services relative to the previous run of the monitor. For example, if the monitor is set to signal an error if a service has changed from running to not running, the monitor only signals an error status for one monitor run cycle. The number of services running and not running is reset for each monitor run and this number is used for comparison with the next monitor run.

### **Configuring the Monitor**

For details on configuring the monitor, see “Microsoft Windows Services State Monitor Settings” on page 727.

## Microsoft Windows Services State Monitor Settings

<b>Description</b>	<p>The Microsoft Windows Services State monitor is used to monitor a list of services running on Windows systems and report changes in the number of services that are running and list the services that changed state.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> </ul>
<b>Included in Tasks</b>	<p>"Deploy a Monitor – Workflow" on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ "Microsoft Windows Services State Monitor Overview" on page 725</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 354.</li> </ul>

## Microsoft Windows Services State Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The Windows server you want to monitor. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>



GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add New Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>
<b>Services to include</b>	<p>Enter an optional regular expression to filter the list of services returned by the monitor. When you use a regular expression to filter the list of services, the monitor calculates changes in state (that is, running or not running) based only on the services matched by the regular expression.</p> <p><b>Default value:</b> <code>/(.*)/</code> (All of the services detected on the remote machine)</p> <p><b>Examples:</b> <code>/.*Network.*/</code> includes all services that contain the word Network.</p>

GUI Element	Description
<p><b>Services to ignore</b></p>	<p>Enter an optional regular expression to filter the list of services matched by the expression used in the <b>Services to include</b> setting. When you use a <b>Services to ignore</b> regular expression to filter the list of <b>Services to include</b>, the monitor calculates changes in state (that is, running or not running) based only on the services matched by the <b>Services to ignore</b> regular expression.</p> <p><b>Examples:</b> <code>/.*Remote.*/</code> ignores all services that contain the word Remote (the services that are ignored are listed in the <b>Services Deleted</b> field).</p>
<p><b>Include driver services</b></p>	<p>Select this box to have the monitor include all low-level driver services. This generally increases the size of the list. You use the <b>Services to include</b> and <b>Service to ignore</b> options to filter the list of services returned using this option.</p>

# 60

---

## Multi Log File Monitor

This chapter includes the main concepts and reference information for the Multi Log File monitor.

### **This chapter includes:**

#### Concepts

- ▶ Multi Log File Monitor Overview on page 731

#### Reference

- ▶ Multi Log Monitor Settings on page 732

### Multi Log File Monitor Overview

---

**Note:** This monitor is available only when SiteScope is configured with System Health.

---

The Multi Log File monitor performs the same functionality as the Log File monitor, but also enables you to run the monitor on all files in a given directory. You specify the directory in the **Log File directory** field in the New Multi Log Monitor dialog box.

For details on configuring the monitor, see “Multi Log Monitor Settings” on page 732.

 **Multi Log Monitor Settings**

<b>Description</b>	<p>The Multi Log monitor checks for specific entries added to a log file by looking for entries containing a text phrase or a regular expression.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This monitor is available only when SiteScope is configured with System Health.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Multi Log File Monitor Overview” on page 731</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Multi Log Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	The server where the files you want to monitor are located.
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>

GUI Element	Description
<p><b>Log file directory</b></p>	<p>Enter the path to the log file you want to monitor. The monitor runs on all files in the directory.</p> <ul style="list-style-type: none"> <li>▶ For reading log files on remote UNIX machines, the path must be relative to the home directory of the UNIX user account being used to log into the remote machine.</li> <li>▶ For reading log files on remote Windows NT/2000 servers using the NetBIOS method, use UNC to specify the path to the remote log file.  <b>Example:</b> \\remoteserver\sharedfolder\filename.log</li> <li>▶ For reading log files on remote Windows NT/2000 servers using the SSH method, specify the local path of the remote log file on the remote machine.  <b>Example:</b> C:\Windows\System32\filename.log</li> </ul> <p>You must also select the corresponding remote Windows SSH server in the <b>Servers</b> box. For details on configuring a remote Windows server for SSH, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p> <p>You can also monitor files local to the server where SiteScope is running.  <b>Example:</b> C:\application\appLogs\access.log</p> <p>Optionally, you can use special date and time regular expression variables to match log file names that include date and time information. For example, you can use a syntax of <code>s/ex\$shortYear\$\$0month\$\$0day\$.log/</code> to match a current date-coded log file. For details on using regular expressions, refer to “SiteScope Date Variables” on page 274.</p>

GUI Element	Description
<b>Content match</b>	<p>Enter the text to look for in the log entries. You can also use a regular expression in this entry to match text patterns. Unlike the content match function of other SiteScope monitors, the Log File monitor content match is run repeatedly against the most recent content of the target log file until all matches are found. This means the monitor not only reports if the match was found but also how many times the matched pattern was found. To match text that includes more than one line of text, add an s search modifier to the end of the regular expression. For details, see “Using Regular Expressions” on page 261. You can also use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</p> <p><b>Note:</b> If you enter more than four content match values, when you create a report by clicking the monitor title, the report includes only the first four values.</p>
<b>File name match</b>	<p>Enter the file name to look for in the log entries. You can also use a regular expression in this entry to match text patterns.</p>
<b>Search from start</b>	<p>Select to search for the specified content from the beginning of the directory.</p> <p><b>Default value:</b> Cleared</p>
<b>Match value labels</b>	<p>Use this option to enter labels for the matched values found in the target log file. The match value labels are used as variables to access retained values from the <b>Content match</b> expression for use with the monitor threshold settings. Separate multiple labels with a comma (.). The labels are used to represent any retained values from the <b>Content match</b> regular expression in the parameters available for the status threshold settings (Error if, Warning if, and Good if). These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.</p> <p><b>Note:</b> If you enter more than four match values, when you create a report by clicking the monitor title, the report includes only the first four values.</p>





# 61

---

## Network Bandwidth Monitor

This chapter includes the main concepts and reference information for the Network Bandwidth monitor.

### **This chapter includes:**

- ▶ Network Bandwidth Monitor Overview on page 737

### **Reference**

- ▶ Network Bandwidth Monitor Settings on page 739

### **Network Bandwidth Monitor Overview**

Use the Network Bandwidth monitor to monitor SNMP-enabled network appliances such as routers and switches. The Network Bandwidth monitor operates like many other browsable monitors to gather information from a source and enable the user to choose which items in the tree it should monitor. It works by connecting to the specified network component and returning a list of interfaces.

The MIB files in `<SiteScope root directory>\templates.mib` are used to create a browsable tree that contains names and descriptions of the objects found during the traversal. Note that an object may or may not be displayed with a textual name and description, depending on the MIBs available in `<SiteScope root directory>\templates.mib`. SiteScope does not display objects for user selection when it has no knowledge of how to display those objects. For example, a plain OctetString may contain binary or ascii data, but SiteScope has no way to decode and display this data correctly without more information.

This section also includes:

- “Performing Sanity Checks” on page 738
- “Configuring the Monitor” on page 738

## Performing Sanity Checks

By default, SiteScope performs a sanity check for every run of the monitor. This checks that the values returned by the monitor are in the valid range. You can also choose to disable these sanity checks.

To disable the sanity checks, clear the **Network Bandwidth monitor sanity check** box in the Infrastructure Settings Preferences page (**Preferences > Infrastructure Settings Preferences > Monitor Settings**).

## Configuring the Monitor

For details on configuring the monitor, see “Network Bandwidth Monitor Settings” on page 739.

## Network Bandwidth Monitor Settings

<b>Description</b>	<p>You use the Network Bandwidth monitor to monitor SNMP-enabled network appliances such as routers and switches. The error and warning thresholds for the monitor can be set on one or more different objects. This monitor type also provides a Real-time metrics report, available as a link in the More column on the Group Detail Page.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When working in template mode, the monitor's non-default thresholds are not copied properly to a template.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Network Bandwidth Monitor Overview” on page 737</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Network Bandwidth Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>SNMP Connection Settings</b>	
<b>Server</b>	Enter the name of the server you want to monitor.
<b>SNMP version</b>	Select the version of SNMP to use when connecting. SiteScope supports SNMP versions 1, 2, and 3. Selecting V3 enables you to enter V3 settings in the SNMP V3 settings panel. <b>Default value:</b> V1
<b>Community</b>	Enter the community string (valid only for version 1 or 2 connections). <b>Default value:</b> public
<b>Timeout (seconds)</b>	Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. <b>Default value:</b> 5 seconds
<b>Retries</b>	Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. <b>Default value:</b> 1
<b>Port</b>	Enter the port to use when requesting data from the SNMP agent. <b>Default value:</b> 161

GUI Element	Description
<b>Starting OID</b>	<p>Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered here. You should edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value did not enable retrieving any counters, then you may have to enter a different value.</p> <p><b>Default value:</b> 1</p>
<p><b>V3 SNMP Settings</b> (This panel is enabled only if V3 is selected in the SNMP version field)</p>	
<b>SNMP V3 authentication type</b>	<p>Select the type of authentication to use for version 3 connections.</p> <p><b>Default value:</b> MD5</p>
<b>SNMP V3 user name</b>	<p>Enter the user name for version 3 connections.</p>
<b>SNMP V3 authentication password</b>	<p>Enter the authentication password to use for version 3 connections.</p>
<b>SNMP V3 privacy password</b>	<p>Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.</p>
<b>SNMP V3 context engine ID</b>	<p>Enter a hexadecimal string representing the Context Engine ID to use for this connection.</p>
<b>SNMP V3 context name</b>	<p>Enter the Context Name to use for this connection.</p>
<p><b>Network Counters</b></p>	
<b>Counters</b>	<p>The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.</p>

GUI Element	Description
<p><b>Get Counters</b></p>	<p>Click to open the Get Counters dialog box. Select the counters you want to monitor.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ The counters displayed are those received during the timeout period, and may not include all the counters available on the server. Specifying a longer timeout in the Timeout (seconds) field in the SNMP Connection Settings panel may result in receiving more counters.</li> <li>▶ The total time for receiving the counters may be longer than the timeout specified, due to additional processing time not part of the request/response period.</li> <li>▶ Due to third-party counter restrictions, the total number of counters that can be monitored is limited to 32.</li> </ul>
<p><b>Advanced Network Settings</b></p>	
<p><b>Device type</b></p>	<p>Select an optional device type for device specific monitoring. By specifying a device type, you enable the Network Bandwidth monitor to watch certain device-specific metrics. For information about controlling the metrics associated with these device types and on adding new device types, see the section entitled Device Specific Metrics Config File.</p> <p><b>Default value:</b> Do not monitor device-specific metrics</p>

GUI Element	Description
<b>Duplex or half-duplex</b>	<p>Select the duplex state (<b>Half-duplex</b> or <b>Full-duplex</b>) to use when calculating percent bandwidth utilized for all selected interfaces on this device.</p> <p><b>Default value:</b> Full-duplex</p>
<b>Interface index</b>	<p>Metrics for network interfaces on an SNMP-enabled device are presented as a table of management information (the ifTable). Each row corresponds to a different interface. There is no requirement that the mappings from interface-to-row in this table remain constant across device reboots. The Interface Index parameter may help prevent the interfaces SiteScope is monitoring from becoming confused after a device restarts.</p> <p>The three possible options are:</p> <ul style="list-style-type: none"> <li>▶ <b>Indexed by interface name.</b> The ifDescr field of the ifTable is used to maintain monitoring consistency across device reboots.</li> <li>▶ <b>Indexed by physical address.</b> The ifPhysAddr field of the ifTable is used to maintain monitoring consistency across device reboots.</li> <li>▶ <b>Indexed by ifTable row number.</b> SiteScope assumes that the interfaces remain in the same row in the ifTable across device reboots.</li> </ul> <p><b>Note:</b> Some devices (for example, Cisco) may have a configuration option to not jumble the position of interfaces in the ifTable during reboot. This may be the safest option, as not all interfaces may always have a unique ifDescr, and not all interfaces may have an ifPhysAddr (loopback interfaces do not typically have a physical address).</p> <p><b>Default value:</b> Indexed by ifTable row number.</p>
<b>Show bytes in/out</b>	<p>Select this option to display a graph for bytes in/out along with the percent bandwidth utilized on the Real-Time Metrics page.</p> <p><b>Default value:</b> Not selected</p>

GUI Element	Description
<b>Real-Time data vertical axis</b>	Enter the maximum value on the vertical axis for real-time graphs (leave blank to have this automatically calculated by SiteScope).
<b>Real-Time data time window (hours)</b>	Enter the number of hours for which real-time graph data should be stored. <b>Default value:</b> 24 hours



# 62

---

## News Monitor

This chapter includes the main concepts and reference information for the News monitor.

### **This chapter includes:**

#### Concepts

- News Monitor Overview on page 745

#### Reference

- News Monitor Settings on page 747

### **News Monitor Overview**

Use the News monitor to regularly monitor news groups on News servers. This enables you to manage the number of articles that are allowed to queue up, and delete them before they cause disk space problems.

This section also includes:

- “Status” on page 746
- “Configuring the Monitor” on page 746

## Status

Each time the News monitor runs, it returns a status message and writes it in the monitoring log file. It also writes the total time it takes to receive a response from the news server, and the number of articles available for each of the specified news groups.

The reading is the current value of the monitor. The possible values for the News monitor are:

- OK.
- unknown host name.
- unable to reach server.
- unable to connect to server.
- timed out reading.
- <news group> not found. The given news group was not found on the news server.
- permission denied for connection. The connection could not be made, probably because the news server was configured to enable connections from a limited range of addresses.
- login expected. The news server expected a user name and password, but none were provided. In this case, enter a user name and password under the Monitor Settings section of the monitor.
- login failed, unauthorized. The user name and password were not accepted by the news server.

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than **OK**.

## Configuring the Monitor

For details on configuring the monitor, see “News Monitor Settings” on page 747.

 **News Monitor Settings**

<b>Description</b>	<p>The News monitor verifies that a news server can be connected to, and is responding. It also measures how long it takes to make a connection, and how many articles are currently in the specified news groups.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>News Server Tool</b> is available when configuring this monitor to access a news server and view the NNTP interaction between SiteScope and the news server (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “News Server Tool” on page 221.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “News Monitor Overview” on page 745</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## News Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>News server</b>	Enter the IP address or the name of the news server that you want to monitor. <b>Example:</b> 206.168.191.21 or news.thiscompany.com. If the port is not the standard news port, add the port after the server with a colon. <b>Example:</b> news.thiscompany.com:7777
<b>News groups</b>	Optionally enter one or more news groups to be checked, separated by commas. Each of these news groups are checked for the current number of articles available in that news group. The reading of the monitor is the sum of articles available for each of the specified news groups.
<b>User name</b>	If your News server requires authorization, enter a valid user name here.
<b>Password</b>	If your News server requires authorization, enter a valid password here.
<b>Advanced Settings</b>	
<b>Connect from</b>	The name or IP address of the server that connects to the News monitor.
<b>Timeout (seconds)</b>	The number of seconds that the News monitor should wait for all of news transactions to complete before timing-out. Once this time period passes, the News monitor logs an error and reports an error status. <b>Default value:</b> 60 seconds

# 63

---

## Oracle 10g Application Server Monitor

This chapter includes the main concepts and reference information for the Oracle 10g Application Server monitor.

**This chapter includes:**

**Concepts**

- ▶ Oracle 10g Application Server Monitor Overview on page 750

**Reference**

- ▶ Oracle 10g Application Server Monitor Settings on page 751

## Oracle 10g Application Server Monitor Overview

Use the Oracle 10g Application Server monitor to monitor the server performance data for Oracle 10g application servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Oracle 10g Application Server in your environment.

---

**Note:** By default, the Oracle 10g metrics servlet is visible only to the local host. To enable monitoring the Oracle 10g Application Server, the servlet must be accessible from other IP addresses. You must edit the **dms.conf** file in the **<Oracle 10g installation path>infra/Oracle/Oracle/conf** directory. For details on editing the file and making this change, refer to the Oracle 10g Application Server documentation. Once configured properly, you should be able to see the following URL: **http://<Oracle 10g machine URL>:7201/dmsoc4j/Spy?format=xml**.

---

For details on configuring the monitor, see “Oracle 10g Application Server Monitor Settings” on page 751.

## Oracle 10g Application Server Monitor Settings

<b>Description</b>	<p>The Oracle 10g Application Server monitor enables you to monitor the availability and performance statistics of an Oracle 10g Application Server. The error and warning thresholds for the monitor can be set on one or more Oracle 10g server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Oracle 10g Application Server Monitor Overview” on page 750</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### Oracle 10g Application Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Authorization user name</b>	If the server you want to monitor requires a name and password for accessing, enter the name.
<b>Authorization password</b>	If the server you want to monitor requires a name and password for accessing, enter the password.

GUI Element	Description
<b>Proxy server</b>	Optionally, a proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.
<b>Proxy server user name</b>	If the proxy server requires a name and password to access the server, enter the name here. Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	If the proxy server requires a name and password to access the server, enter the password here. Your proxy server must support Proxy-Authenticate for these options to function.
<b>Host name</b>	Enter the server administration URL for the server you want to monitor.
<b>Metric type</b>	Enter the type of metrics to monitor. Options are App Server (OC4J) and Web Server (DMS).
<b>Port</b>	Enter the server port for the server you want to monitor. <b>Default value:</b> 7201 (configured in the <b>dms.conf</b> file)
<b>Secure server</b>	Select this option to use a secure server.
<b>Timeout (seconds)</b>	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status. <b>Default value:</b> 60 seconds
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor. <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.



# 64

---

## Oracle 9i Application Server Monitor

This chapter includes the main concepts and reference information for the Oracle 9i Application Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ Oracle 9i Application Server Monitor Overview on page 753

#### Reference

- ▶ Oracle 9i Application Server Monitor Settings on page 754

### **Oracle 9i Application Server Monitor Overview**

Use the Oracle 9i Application Server monitor to monitor the server performance data for Oracle 9i servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Oracle 9i Application server in your environment.

---

**Note:** You must enable Web caching on the Oracle 9i Application Server to use the Oracle 9i Application Server monitor.

---

For details on configuring the monitor, see “Oracle 9i Application Server Monitor Settings” on page 754.



## Oracle 9i Application Server Monitor Settings

<b>Description</b>	<p>The Oracle 9i Application Server monitor enables you to monitor the availability and performance statistics of a Oracle 9i Application Server. The error and warning thresholds for the monitor can be set on one or more Oracle 9i server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ The <b>URL Tool</b> is available when configuring this monitor to request a URL from a server, print the returned data, and test network routing (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “URL Tool” on page 247.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Oracle 9i Application Server Monitor Overview” on page 753</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Oracle 9i Application Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>URL</b>	Enter the server administration URL for the server you want to monitor. The URL is usually in the format: <code>http://server:port/webcacheadmin?SCREEN_ID=CGA.Site.Stats&amp;ACTION=Show</code> .
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.
<b>Authorization user name</b>	If the server you want to monitor requires a name and password for access, enter the name.
<b>Authorization password</b>	If the server you want to monitor requires a name and password for access, enter the password.
<b>HTTP Proxy</b>	Optionally, a proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.
<b>Proxy user name</b>	If the proxy server requires a name and password to access the server, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy password</b>	If the proxy server requires a name and password to access the server, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
<b>Timeout (seconds)</b>	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.



# 65

---

## Oracle Database Monitor

This chapter includes the main concepts and reference information for the Oracle Database monitor.

### **This chapter includes:**

#### Concepts

- ▶ Oracle Database Monitor Overview on page 757

#### Reference

- ▶ Oracle Database Monitor Settings on page 760

### Oracle Database Monitor Overview

Use the Oracle Database monitor to monitor the server performance statistics from Oracle Database 8i, 9i, 10g and 11g servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate Oracle Database monitor instance for each Oracle database server in your environment.

---

**Note:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of an Oracle database server. For details, see “Oracle Database Solution Template” on page 1759.

---

This section contains the following topics:

- “Setup Requirements and User Permissions” on page 758
- “Oracle Database Topology Settings” on page 759
- “Configuring the Monitor” on page 760

## Setup Requirements and User Permissions

The following are several key requirements for using the Oracle Database monitor:

- You must have a copy of the applicable Oracle JDBC database driver file (for example, `classes12.zip`) on the SiteScope server. Copy the downloaded driver file into the `<SiteScope root directory>\WEB-INF\lib` subdirectory. Do not unzip the file. Stop and restart the SiteScope service after copying the driver file to the SiteScope machine.

---

**Note:** More than one driver file is available for download. Some drivers support more than one version of Oracle database (for example, the `classes12.zip` Oracle JDBC thin driver) while others only support a particular version. If you are monitoring a recent version of Oracle database, download the latest version of the database driver.

---

- You must supply the correct **Database connection URL**, a database user name and password when setting up the monitor. When using the Oracle thin driver, the database connection URL has the form of:  
`jdbc:oracle:thin:@<server name or IP address>:<port>:<database sid>`.

For example, to connect to the ORCL database on a machine using port 1521 you would use:

`jdbc:oracle:thin:@206.168.191.19:1521:ORCL`.

---

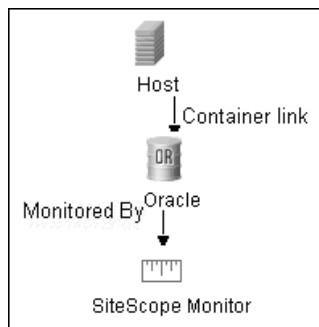
**Note:** The colon (:) and the at (@) symbols must be included as shown.

---

- ▶ You must know the syntax for accessing the Oracle **Database driver** that was installed on the SiteScope server. Examples of common database driver strings are:
  - ▶ **com.inet.ora.OraDriver.** A driver from Oracle for Oracle databases. This driver is deployed with SiteScope.
  - ▶ **oracle.jdbc.driver.OracleDriver.** JDBC thin driver for Oracle 7 and 8 databases. This driver is an Oracle product and is supplied by Oracle.
  - ▶ **com.mercury.jdbc.oracle.OracleDriver.** A driver for Oracle databases. This driver is deployed with SiteScope. When using the Oracle mercury driver, the database connection URL has the form of:  
`jdbc:mercury:oracle://<server name or IP address>:<database server port>;sid=<sid>`
- ▶ You should have only one version of each driver installed on the SiteScope machine. If there is more that version is installed, SiteScope may report an error and be unable to connect to the database.
- ▶ The user specified in the **Credentials** section must be granted the permission to access System tablespace.

## Oracle Database Topology Settings

The Oracle Database monitor can identify the topology of the Oracle databases being monitored. If **Include topology data when reporting to HP Business Availability Center** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



To ensure that the topology is reported accurately, you should enter the values for the **Database machine name** and the **SID**. These fields appear in the **HP BAC Integration Settings** under **Topology Settings**.

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160.

## Configuring the Monitor

For details on configuring the monitor, see “Oracle Database Monitor Settings” on page 760.

## Oracle Database Monitor Settings

<p><b>Description</b></p>	<p>The Oracle Database monitor enables you to monitor the availability of an Oracle database server (versions 9i plus some earlier versions). The error and warning thresholds for the monitor can be set on one or more Oracle server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ If you are using a third-party database driver and you upgrade SiteScope, you must deploy the driver to SiteScope again, since the driver configuration data is not saved during an upgrade.</li> </ul>



<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Oracle Database Monitor Overview” on page 757</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Oracle Database Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Database connection URL</b>	<p>Enter the connection URL to the database you want to connect to. The syntax is <code>jdbc:oracle:thin:@&lt;server name or IP address&gt;:&lt;database server port&gt;;sid=&lt;sid&gt;</code>.</p> <p><b>Example:</b> To connect to the ORCL database on a machine using port 1521, use: <code>jdbc:oracle:thin:@206.168.191.19:1521:ORCL</code>.</p> <p><b>Note:</b> The colon (:) symbol must be included as shown.</p>
<b>Database driver</b>	<p>Enter the driver used to connect to the database.</p> <p><b>Example:</b> <code>oracle.jdbc.driver.OracleDriver</code></p>
<b>Credentials</b>	<p>Select the option for providing the user name and password to be used to access the database server.</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>

GUI Element	Description
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.

### Database Connection Settings

<b>Description</b>	<p>The Database Connection Settings enable you to retrieve, share, and reuse database connections for database monitors that use any JDBC-compliant driver. When multiple database monitors use the same database, using a connection pool instead of an open connection for each monitor improves monitor performance and optimizes database server resource utilization.</p> <p>Connections can be shared regardless of monitor type. For example, SiteScope database logger, database tools (Database Connection, Database Information), database alerts, and database monitors (Oracle Database, Database Counter, Database Query, DB2 8 and 9, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>
<b>Important Information</b>	You can set additional database options that affect all resources that connect to the database in the JDBC Global Options in the General Preferences container.
<b>Useful Links</b>	“JDBC Global Options” on page 1386

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Use connection pool</b>	<p>Enables SQL connection sharing. This means that you use a connection pool rather than open and close a new connection for each monitor query.</p> <p><b>Default value:</b> Selected</p>
<b>Physically close if idle connection count exceeds</b>	<p>The maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool.</p> <p><b>Default value:</b> 10</p>
<b>Idle connection timeout</b>	<p>The maximum amount of time, in seconds/minutes/hours/days, that a SQL connection remains unused after it has been returned to the SQL connection pool. When the time is exceeded, the connection is automatically closed.</p> <p><b>Default value:</b> 5 minutes</p>
<b>Query timeout</b>	<p>The amount of time, in seconds/minutes/hours/days, to wait for execution of a SQL statement. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored.</p> <p><b>Default value:</b> 1 minute</p>

## HP BAC Integration Settings - Topology Settings

**Note:** The HP BAC Integration Settings panel is displayed only when SiteScope is reporting to HP Business Availability Center.

<b>Description</b>	Use the HP BAC Integration Settings area to control what data a monitor forwards to the HP Business Availability Center database. The topology settings for the Oracle Database monitor include fields that must be entered to ensure that the topology SiteScope reports to HP Business Availability Center.
<b>Important Information</b>	The monitor specific settings are described below. For details on the HP BAC Integration Settings common to all monitors, see “Common Monitor Settings” on page 354.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Database machine name</b>	Enter the database machine name to enable accurate reporting of CI property information to HP Business Availability Center from the monitored Oracle database. If this field is left empty and the monitor cannot discover the database machine name, the CI data may not be reported accurately.
<b>SID</b>	Enter the SID to enable accurate reporting of CI property information to HP Business Availability Center from the monitored Oracle database. If this field is left empty and the monitor cannot discover the SID, the CI data may not be reported accurately.

# 66

---

## Ping Monitor

This chapter includes the main concepts and reference information for the Ping monitor.

### **This chapter includes:**

#### Concepts

- ▶ Ping Monitor Overview on page 765

#### Reference

- ▶ Ping Monitor Settings on page 767

### Ping Monitor Overview

The Ping monitor obtains two of the most common measurements used to determine if your network connection is congested: Round Trip Time and Loss Percentage. An increase of either of these suggests that you are experiencing problems.

In the case of Loss Percentage, you want to see a 0% reading. A 100% reading indicates your link is completely down. Some loss may happen occasionally, but if it becomes common, either some packets are being lost or the router is exceptionally busy and dropping packets.

Each time the Ping monitor runs, it returns a reading and a status message and writes them in the monitoring log file. It also writes the total time it takes to receive a response from the designated host in the log file.

This section contains the following topics:

- “What to Monitor” on page 766
- “Scheduling the Monitor” on page 766
- “Troubleshooting and Limitations” on page 766
- “Configuring the Monitor” on page 767

## **What to Monitor**

We recommend that you set up monitors that test your connection to the Internet at several different points. For example, if you have a T1 connection to a network provider who in turn has a connection to the backbone, you would want to set up a Ping monitor to test each of those connections. The first monitor would ping the router on your side of the T1. The second would ping the router on your provider's side of the T1. The third monitor would ping your provider's connection to the backbone.

In addition to these monitors, it is also a good idea to have a couple of other monitors ping other major network providers. These monitors do not really tell you whether the other provider is having a problem, but it does tell you if your network provider is having trouble reaching them.

## **Scheduling the Monitor**

You can monitor your own router as often as every two minutes without compromising system performance. The monitors that watch your provider's connection to your line and to the backbone should only be run every ten minutes or so. This minimizes traffic while still providing you with sufficient coverage.

## **Troubleshooting and Limitations**

If you are unable to ping a remote machine, there are several possible causes:

- If you are trying to ping a host name, make sure the name you are pinging is fully qualified.
- If pinging the fully qualified host name does not work, try pinging the IP address of the destination machine. If ping fails when you try the name of the site, but works when you try the IP address, it is a problem with DNS.

- If pinging both the name and the IP address fail, it might be because they are administratively denied by an access control list. Sometimes routers block ping with an access list. Try a traceroute instead, or if it is a Web site, try browsing it.
- If the traceroute shows multiple hops between you and the destination, try pinging each host in the path. Start pinging the host closest to you, and work your way towards the destination until you find the host that fails to respond to ping. Use a traceroute to get a list of the hosts between you and the destination for this purpose.

## Configuring the Monitor

For details on configuring the monitor, see “Ping Monitor Settings” on page 767.

## Ping Monitor Settings

<p><b>Description</b></p>	<p>The Ping monitor checks the availability of a host by using ICMP (Internet Control Message Protocol). Use this monitor to check network connectivity and response time.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>➤ Monitors must be created in a group in the monitor tree.</li> <li>➤ The <b>Ping Tool</b> is available when configuring this monitor to check if the host can be reached, and the round-trip time along the path (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Ping Tool” on page 226.</li> </ul>

<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Ping Monitor Overview” on page 765</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### Ping Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Host</b>	<p>Enter the IP address or the name of the host that you want to monitor.</p> <p><b>Example:</b> 206.168.191.21 or demo.thiscompany.com</p> <p><b>Note:</b> You can monitor only one IP or host name at a time for each monitor instance.</p>
<b>Packet size (bytes)</b>	<p>The size, in bytes (including the IP and ICMP headers), of the ping packets sent. To change the threshold, enter the new value in the text box.</p> <p><b>Default value:</b> 32 bytes</p>
<b>Timeout (milliseconds)</b>	<p>The time, in milliseconds, that should pass before the ping times out. To change the threshold, enter the new value in the text box.</p> <p><b>Default value:</b> 5000 milliseconds</p>



# 67

---

## Port Monitor

This chapter includes the main concepts and reference information for the Port monitor.

### **This chapter includes:**

#### Concepts

- ▶ Port Monitor Overview on page 769

#### Reference

- ▶ Port Monitor Settings on page 771

### **Port Monitor Overview**

Use the Port monitor for monitoring network applications that none of the other SiteScope monitors watch such as Gopher and IRC services, some media services, or other custom network applications. You are notified immediately if SiteScope is unable to connect to the monitored port.

This section contains the following topics:

- ▶ “Status” on page 770
- ▶ “Scheduling the Monitor” on page 770
- ▶ “Configuring the Monitor” on page 770

## Status

Each time the Port monitor runs, it returns a status message and writes it in the monitoring log file. It also writes the total time it takes to receive a response from the remote service.

The reading is the current value of the monitor. The possible values for the Port monitor are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- match error

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

## Scheduling the Monitor

Scheduling Port monitors depends on the application or system you are monitoring. The Port monitor does not use many resources, so you can schedule it to run as often as every 15 seconds if necessary. Monitoring most systems every 10 minutes is normally sufficient.

## Configuring the Monitor

For details on configuring the monitor, see “Port Monitor Settings” on page 771.

 **Port Monitor Settings**

<b>Description</b>	<p>The Port monitor verifies that a connection can be made to a network port and measures the length of time it takes to make the connection. Optionally, it can look for a string of text to be returned or send a string of text once the connection is made.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>Ping Tool</b> is available when configuring this monitor to check if the host can be reached, and the round-trip time along the path (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Ping Tool” on page 226.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Port Monitor Overview” on page 769</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Port Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Host name</b>	Enter the IP address or the name of the host that you want to monitor. <b>Example:</b> 206.168.191.21 or demo.thiscompany.com
<b>Port number</b>	Choose the port number to connect to from the list of <b>Commonly used ports</b> , or enter a port number in the <b>Other ports</b> text box. Additional entries can be added to the list by editing the <code>&lt;SiteScope root directory&gt;\groups\master.config</code> file.
<b>Timeout (seconds)</b>	The number of seconds that the Port monitor should wait for the connection to the port, and for any sending and receiving to complete. Once this time period passes, the Port monitor logs an error and reports an error status. <b>Default value:</b> 60 seconds
<b>Send string</b>	Customize the string sent to the host after a connection is made.
<b>Match string</b>	Check for a string of text after a connection is made. If the text is not received, the monitor displays the message no match on content. <b>Note:</b> <ul style="list-style-type: none"> <li>▶ The search is case sensitive.</li> <li>▶ You cannot use regular expressions in this field.</li> </ul>

# 68

---

## Radius Monitor

This chapter includes the main concepts and reference information for the Radius monitor.

### **This chapter includes:**

#### Concepts

- ▶ Radius Monitor Overview on page 773

#### Reference

- ▶ Radius Monitor Settings on page 775

### **Radius Monitor Overview**

Use the Radius monitor to test that the RADIUS server correctly handles authentication requests. If the RADIUS server fails, any users that try to use it are unable to login and access any services. Create a separate monitor instance for each server you are running. You may want to setup multiple monitors per server if you want to test different kinds of login accounts.

This section contains the following topics:

- ▶ “Setup Requirements” on page 774
- ▶ “Status” on page 774
- ▶ “Configuring the Monitor” on page 774

## Setup Requirements

- For SiteScope to monitor your RADIUS server, you must first add the IP address of your SiteScope server to the list of Clients that the RADIUS server is allowed to communicate with. This must be done in order for the Radius Server to take requests from SiteScope. Failure to do this results in Unknown Client errors on the RADIUS server.
- The Radius monitor currently supports Password Authentication Procedure (PAP) authentication but not the Challenge Handshake Authentication Protocol (CHAP) or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). Your RADIUS server must be configured to accept PAP requests to use this monitor.

## Status

Each time the Radius monitor runs, it returns a status message and writes it in the monitoring log file. It also writes the total time it takes to receive a authentication response. The reading is the current value of the monitor. The possible values for the Radius monitor are:

- OK
- unknown host name
- timed out reading
- match error

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than **OK**.

## Configuring the Monitor

For details on configuring the monitor, see “Radius Monitor Settings” on page 775.

## Radius Monitor Settings

<b>Description</b>	<p>The Radius (Remote Authentication Dial In User Service) monitor checks that a RADIUS server is working correctly by sending an authentication request and checking the result.</p> <p>A RADIUS server is used to authenticate users, often connecting through a remote connection such as a dialup modem or a DSL line.</p> <p>Use this page to add a monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.
<b>Included in Tasks</b>	"Deploy a Monitor – Workflow" on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ "Radius Monitor Overview" on page 773</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 354.</li> </ul>

### Radius Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Radius server</b>	Enter the IP address or the name of the RADIUS server that you want to monitor. <b>Example:</b> 206.168.191.21 or radius.thiscompany.com
<b>Secret phrase</b>	Enter the secret used to encrypt all requests to this RADIUS server.
<b>User name</b>	Enter the user name to authenticate.
<b>Password</b>	Enter the password to authenticate.

GUI Element	Description
<b>Timeout (seconds)</b>	<p>The number of seconds that the Radius monitor should wait for the connection to the port, and for any sending and receiving to complete.</p> <p>Once this time period passes, the Radius monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 30 seconds</p>
<b>Port</b>	<p>Choose the UDP port used by the RADIUS server.</p> <p><b>Default value:</b> 1645</p>
<b>Match content</b>	<p>Enter a string of text to check for in the response. If the text is not contained in the response, the monitor displays the message <b>no match on content</b>.</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p><b>Example:</b> <code>/\d\d/</code> or <code>/size \d\d/i</code></p> <p><b>Note:</b> The search is case sensitive.</p>



# 69

---

## Real Media Player Monitor

This chapter includes the main concepts and reference information for the Real Media Player monitor.

### **This chapter includes:**

#### Concepts

- ▶ Real Media Player Monitor Overview on page 777

#### Reference

- ▶ Real Media Player Monitor Settings on page 779

### **Real Media Player Monitor Overview**

Use the Real Media Player monitor to monitor availability and delivery quality parameters for media files and streaming data compatible with RealNetworks Real Media Player versions 7.x, 8.x, 9.x, and 10.x. You can monitor multiple parameters or counters with a single monitor instance. This enables you to report on delivery performance. Create a separate monitor instance for files or data streams that are representative of the content available from the site you want to monitor.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only.

---

This section also includes:

- “Setup Requirements” on page 778
- “Configuring the Monitor” on page 778

### **Setup Requirements**

Before you can use the Real Media Player monitor, Real Media Player client libraries must be installed on the server where SiteScope is running. Normally, it is sufficient to download and install a Real Media Player client on the server.

### **Configuring the Monitor**

For details on configuring the monitor, see “Real Media Player Monitor Settings” on page 779.



## Real Media Player Monitor Settings

<b>Description</b>	<p>The Real Media Player monitor enables you to emulate a user playing media or streaming data from a Real Media Server.</p> <p>The error and warning thresholds for the monitor can be set on one or more Real Media Player performance statistics.</p> <p>This monitor does not support metadata files such as the .smi format.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>Real Media Player Tool</b> is available when configuring this monitor (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Real Media Player Tool” on page 230.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Real Media Player Monitor Overview” on page 777</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Real Media Player Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>URL</b>	<p>Enter the URL of the media file or streaming source you want to monitor. This should be the URL of the media file.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ Only monitor video, not audio, streams with this monitor.</li> <li>▶ This monitor does not support metadata files such as the .smi format.</li> </ul>
<b>Duration (seconds)</b>	<p>Enter the playback duration that the monitor should use for the media file or source. The duration value does not need to match the duration of the media contained in the file.</p> <p>If the media content of the file or source you are monitoring is less than the duration value selected for the monitor, the monitor plays the entire media content and reports the results, including the time required to play the media content.</p> <p><b>Default value:</b> 15 seconds</p>
<b>Counters</b>	<p>Select the server performance counters you want to check with this monitor. The list displays the available counters and those currently selected for this monitor.</p>

# 70

---

## Real Media Server Monitor

This chapter includes the main concepts and reference information for the Real Media Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ Real Media Server Monitor Overview on page 781

#### Reference

- ▶ Real Media Server Monitor Settings on page 783

### **Real Media Server Monitor Overview**

Use the Real Media Server monitor to monitor the server performance parameters for RealNetworks Real Media Servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each RealSystem Server you are running.

**Note:**

- ▶ This monitor is supported in SiteScopes that are running on Windows versions only.
  - ▶ By default, SiteScope monitors the Real Media Server default service, **RMServer**. To monitor other services, add the service names (separated by commas) to the **Real Media Server monitor service names** box in **Preferences > Infrastructure Preferences > Monitor Settings**.
- 

This section also includes:

- ▶ “Setup Requirements and User Permissions” on page 782
- ▶ “Configuring the Monitor” on page 782

## **Setup Requirements and User Permissions**

The following are key requirements for using the Real Media Server monitor:

- ▶ The Real Media Server monitor makes use of Performance Counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you must define the connection to these servers under the Microsoft Windows Remote Servers container in the remote server tree.
- ▶ The Remote Registry service must be running on the machine where the Real Media server is running if the Real Media Server is running on Windows 2000.

## **Configuring the Monitor**

For details on configuring the monitor, see “Real Media Server Monitor Settings” on page 783.

## Real Media Server Monitor Settings

<p><b>Description</b></p>	<p>The Real Media Server monitor enables you to monitor the availability of a Real Media Server on Windows NT systems.</p> <p>The error and warning thresholds for the monitor can be set on one or more Real Media Server performance statistics.</p> <p>Use this page to add a monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Real Media Server Monitor Overview” on page 781</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Real Media Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the Real Media Server you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>



GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p>
<b>Counters</b>	<p>The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p><b>Note when working in template mode:</b> To update counters in template browsable monitors that need a target server, click the <b>Select measurement from</b> button and add the required server and counters. Any server that is accessible in the domain can be used. If a server is not in the domain, you must manually add the server to the remote server tree before adding counters, and then specify the newly created server name in the <b>Server</b> field.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p>



# 71

---

## SAP CCMS Monitor

This chapter includes the main concepts, tasks, and reference information for the SAP CCMS monitor.

### **This chapter includes:**

#### **Concepts**

- ▶ SAP CCMS Monitor Overview on page 788

#### **Tasks**

- ▶ Configure the SAP CCMS Monitoring Environment on page 792

#### **Reference**

- ▶ SAP CCMS Monitor Settings on page 795

## SAP CCMS Monitor Overview

Use the SAP CCMS monitor to retrieve and report metrics using SAP's centralized monitoring architecture, CCMS (Computer Center Management System). With CCMS, a SAP administrator can monitor all servers, components and resources in the R/3 4.6B, R/3 4.6C, R/3 4.7E, SAP ECC5 and SAP ECC6 landscape from a single centralized server, greatly facilitating not only problem discovery but also problem diagnosis.

---

### Note:

- ▶ The SAP CCMS monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a SAP CCMS environment. For details, see “SAP Solution Templates” on page 1769.

---

Using the SAP CCMS monitor, you can also enable reporting of the host topology to Business Availability Center. If enabled, Business Availability Center automatically populates the CMDB with CIs based on the monitored hardware in SiteScope.

Using SAP's advanced CCMS interface BC-XAL 1.0, the SiteScope SAP CCMS monitor exposes hundreds of performance and availability metrics. The error and warning thresholds for the monitor can be set for one or more of the nearly 120 SAP server performance statistics available by using the CCMS interface.

This section contains the following topics:

- ▶ “Setup Requirements and User Permissions” on page 789
- ▶ “SAP CCMS Topology Settings” on page 790
- ▶ “Troubleshooting and Limitations” on page 791
- ▶ “Configuring the Monitor” on page 792

## Setup Requirements and User Permissions

The following are requirements for using the SAP CCMS monitor

- ▶ The SAP Java Connector (SAP JCo 2.0.6 and later) component must be downloaded from the SAP Service Marketplace Software Distribution Center, and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

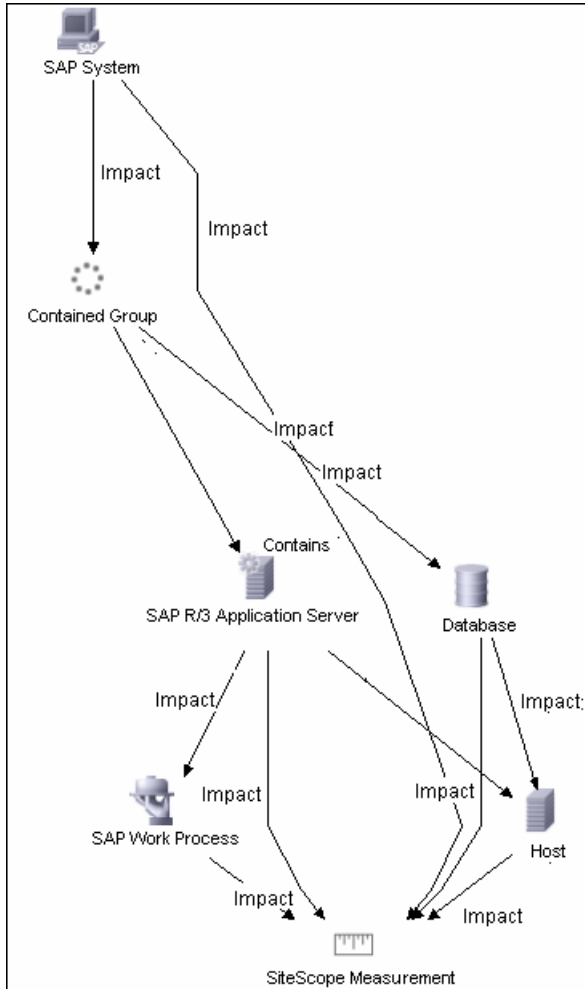
For details on downloading the SAP Java Connector and enabling the monitor, see “Configure the SAP CCMS Monitoring Environment” on page 792.

- ▶ The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and above only.
- ▶ Consult your SAP documentation to determine if your R/3 landscape components may need additional software installed to run or work with CCMS.
- ▶ A SAP user requires certain privileges to read CCMS metrics. When defining a SAP CCMS monitor in SiteScope you must specify a user who has XMI authorization to be able to login to the CCMS server and retrieve metrics. The user should have one or more of the profiles listed below assigned to it. Authorizations are collected in SAP profiles, and the following profiles include XMI authorization:
  - ▶ S\_A.SYSTEM
  - ▶ PD\_CHICAGO
  - ▶ S\_WF\_RWTEST
  - ▶ SAP\_ALL

One test to see if a user has such authorization is to try and issue transaction RZ20 in the SAP GUI and see if the CCMS monitor sets can be displayed.

## SAP CCMS Topology Settings

The SAP CCMS monitor can identify the topology of the SAP System being monitored. If **Include topology data when reporting to BAC** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the Universal CMDB as SiteScope Measurement Groups and SiteScope Measurement CIs.

---

**Note:**

- ▶ This direct integration between SiteScope and Business Availability Center is available only when the Business Availability Center for SAP Applications license is installed.
  - ▶ When you add a new application server to the SAP System, you must clear the **Report SAP topology to HP Business Availability Center** option, save the monitor definition, and then select the option again and save the monitor definition, in order for the monitor to recognize the new application server.
- 

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160 in the HP Business Availability Center Documentation Library.

For information about the SAP topology, see “SAP Systems View” in *Solutions and Integrations* in the HP Business Availability Center Documentation Library.

**Troubleshooting and Limitations**

- ▶ The SAP CCMS monitor only retrieves and displays numeric metrics (Performance attributes). Status, Log and Information attributes are not supported. Also, presentation and management of SAP CCMS Alerts in SiteScope are not supported at this time.
- ▶ Due to the large amount of metrics that are retrieved when displaying the entire SAP metrics browse tree during monitor definition, there could be a delay in opening the Choose Counters page. However, after a browse tree has been successfully retrieved, it is cached to file automatically, so that the next time you retrieve metrics from the same server/user name, the wait time is greatly reduced.

## Configuring the Monitor

For task details, see “Configure the SAP CCMS Monitoring Environment” on page 792.

For user interface details, see “SAP CCMS Monitor Settings” on page 795.

## Configure the SAP CCMS Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Prerequisites” on page 792
- “Download the SAP Java Connector” on page 793
- “Enable the SAP CCMS Monitor (on a Windows Environment)” on page 793
- “Enable the SAP CCMS Monitor (on a UNIX Environment)” on page 794
- “Configure the Monitor Properties” on page 794

### 1 Prerequisites

A SAP user requires certain privileges to login to the CCMS server and retrieve metrics. For details on this topic, see “Setup Requirements and User Permissions” on page 789.



## 2 Download the SAP Java Connector

The SAP Java Connector (SAP JCo 2.0.6 and above) component must be downloaded and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

- a** To download SAP Java Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>).

---

**Note:** You need a valid Service Marketplace login to access the SAP Web site

---

- b** Click **SAP Java Connector**, and then click **Tools and Services**.

## 3 Enable the SAP CCMS Monitor (on a Windows Environment)

The SAP CCMS monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

- a** Download the following .jar file and .dll files from the SAP support Web site (<http://www.service.sap.com/connectors>):
  - **sapjco.jar**
  - **librfc32.dll**
  - **sapjcorfc.dll**
- b** Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.

- c Copy the two .dll files into the <SiteScope root directory>\bin directory.

---

**Note:** Check if the .dll files already exist in the <Windows installation directory>/system32 directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

---

- d Restart SiteScope.

#### 4 Enable the SAP CCMS Monitor (on a UNIX Environment)

The SAP CCMS monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

- a Download the following .jar file and .so files from the SAP support Web site:
  - **sapjco.jar**
  - **librfccm.so**
  - **libsapjcorfc.so**
- b Copy the **sapjco.jar** file into the <SiteScope root directory>\WEB-INF\lib directory.
- c Copy the two .so files as follows:
  - For Sun installations, copy into the <SiteScope root directory>\java\lib\sparc directory.
  - For Linux installation, copy into the <SiteScope root directory>\java\lib\i386 directory.
- d Restart SiteScope.

#### 5 Configure the Monitor Properties

Complete the SAP CCMS monitor configuration. For details on the monitor settings, see “SAP CCMS Monitor Settings” on page 795.

## SAP CCMS Monitor Settings

<b>Description</b>	<p>The SAP CCMS monitor enables you to monitor the performance of your SAP R/3 System landscape in a centralized manner using SAP CCMS interface.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the SAP CCMS Monitoring Environment” on page 792</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SAP CCMS Monitor Overview” on page 788</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## SAP CCMS Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Application server</b>	Enter the address of the SAP server you want to monitor.
<b>SAP client</b>	Enter the Client to use for connecting to SAP.
<b>System number</b>	Enter the System number for the SAP server.
<b>SAP router string</b>	<p>If your connection is being made through a router, enter a router address string, otherwise leave it blank.</p> <p>You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select <b>Properties</b> to view the router address.</p>
<b>Credentials</b>	<p>Select the option for providing the user name and password to be used to access the SAP server.</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the SAP server in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>

GUI Element	Description
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor. This tree more or less matches the hierarchy of Monitoring Tree Elements displayed in the Monitoring Tree that is shown in the SAP GUI with transaction RZ20. However, the SiteScope browse tree may show more or less information than RZ20 depending on the authorization level of the user name you specified for this monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>



# 72

---

## SAP CCMS Alerts Monitor

This chapter includes the main concepts, tasks, and reference information for the SAP CCMS Alerts monitor.

**This chapter includes:**

**Concepts**

- ▶ SAP CCMS Alerts Monitor Overview on page 800

**Tasks**

- ▶ Configure the SAP CCMS Alerts Monitoring Environment on page 801

**Reference**

- ▶ SAP CCMS Alerts Monitor Settings on page 804

## SAP CCMS Alerts Monitor Overview

Use the SAP CCMS Alerts monitor to retrieve and report alerts from the SAP CCMS monitors using SAP's centralized monitoring architecture, CCMS (Computer Center Management System). The SAP CCMS Alerts monitor retrieves alerts using SAP's advanced CCMS interface BC-XAL 1.0.

The SAP CCMS Alerts monitor enables you to monitor alerts for various components of your SAP R/3 4.6B, R/3 4.6C, R/3 4.7E, and SAP ECC5 and ECC6 landscape.

---

**Note:** The SAP CCMS Alerts monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

---

This section also includes:

- ▶ “Setup Requirements and User Permissions” on page 800
- ▶ “Configuring the Monitor” on page 801

### **Setup Requirements and User Permissions**

- ▶ The SAP CCMS Alerts monitor requires that the SAP Java Connector (SAP JCo 2.0.6 and later) component be downloaded from the SAP Service Marketplace Software Distribution Center, and installed on the same server where SiteScope is running (or at least be accessible on a remote shared location).

For details on downloading the SAP Java Connector and enabling the monitor, see “Configure the SAP CCMS Alerts Monitoring Environment” on page 801.

- ▶ The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and above only.
- ▶ Consult your SAP documentation to determine if your R/3 landscape components may need additional software installed to run or work with CCMS.



- ▶ A SAP user requires certain privileges to read CCMS metrics. When defining a SAP CCMS Alerts monitor in SiteScope you must specify a user who has XMI authorization to be able to login to the CCMS server and retrieve metrics. The user should have one or more of the profiles listed below assigned to it. Authorizations are collected in SAP profiles, and the following profiles include XMI authorization:
  - ▶ S\_A.SYSTEM
  - ▶ PD\_CHICAGO
  - ▶ S\_WF\_RWTEST
  - ▶ SAP\_ALL

One test to see if a user has such authorization is to try and issue transaction RZ20 in the SAP GUI and see if the CCMS monitor sets can be displayed.

### **Configuring the Monitor**

For task details, see “Configure the SAP CCMS Alerts Monitoring Environment” on page 801.

For user interface details, see “SAP CCMS Alerts Monitor Settings” on page 804.

## **Configure the SAP CCMS Alerts Monitoring Environment**

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- ▶ “Prerequisites” on page 802
- ▶ “Download the SAP Java Connector” on page 802
- ▶ “Enable the SAP CCMS Alerts Monitor (on a Windows Environment)” on page 802
- ▶ “Enable the SAP CCMS Alerts Monitor (on a UNIX Environment)” on page 803

- “Configure the Monitor Properties” on page 803

## 1 Prerequisites

A SAP user requires certain privileges to login to the CCMS server and retrieve metrics. For details on this topic, see “Setup Requirements and User Permissions” on page 800.

## 2 Download the SAP Java Connector

The SAP Java Connector (SAP JCo 2.0.6 and above) component must be downloaded and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

- a** To download SAP Java Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>).

---

**Note:** You need a valid Service Marketplace login to access the SAP Web site

---

- b** Click **SAP Java Connector**, and then click **Tools and Services**.

## 3 Enable the SAP CCMS Alerts Monitor (on a Windows Environment)

The SAP CCMS monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

- a** Download the following .jar file and .dll files from the SAP support Web site (<http://www.service.sap.com/connectors>):
  - **sapjco.jar**
  - **librfc32.dll**
  - **sapjcorfc.dll**
- b** Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.

- c Copy the two .dll files into the <SiteScope root directory>\bin directory.

---

**Note:** Check if the .dll files already exist in the <Windows installation directory>/system32 directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

---

- d Restart SiteScope.

#### 4 Enable the SAP CCMS Alerts Monitor (on a UNIX Environment)

The SAP CCMS monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

- a Download the following .jar file and .so files from the SAP support Web site:
  - sapjco.jar
  - librfccm.so
  - libsapjcorfc.so
- b Copy the sapjco.jar file into the <SiteScope root directory>\WEB-INF\lib directory.
- c Copy the two .so files as follows:
  - For Sun installations, copy into the <SiteScope root directory>\java\lib\sparc directory.
  - For Linux installation, copy into the <SiteScope root directory>\java\lib\i386 directory.
- d Restart SiteScope.

#### 5 Configure the Monitor Properties

Complete the SAP CCMS Alerts monitor configuration. For details on the monitor settings, see “SAP CCMS Alerts Monitor Settings” on page 804.

---

**Note:** While you can change the run schedule for this monitor to run more or less often using the **Frequency** setting in Monitor Run Settings (the default is every 10 minutes), CCMS metrics are generally only updated once every 5 minutes.

---

## SAP CCMS Alerts Monitor Settings

<p><b>Description</b></p>	<p>The SAP CCMS Alerts monitor enables you to read and complete alerts from the SAP CCMS Alerts monitors.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “Configure the SAP CCMS Alerts Monitoring Environment” on page 801</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “SAP CCMS Alerts Monitor Overview” on page 800</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## SAP CCMS Alerts Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Application server</b>	Enter the host name/IP address of the SAP server you want to monitor.
<b>SAP client</b>	Enter the Client to use for connecting to SAP.
<b>System number</b>	Enter the System number for the SAP server.
<b>SAP router string</b>	<p>If your connection is being made through a router, enter a router address string, otherwise leave it blank.</p> <p>You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select Properties to view the router address.</p>
<b>Credentials</b>	<p>Select the option for providing the user name and password to be used to access the SAP CCMS metrics.</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the SAP server in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>

GUI Element	Description
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

# 73

---

## SAP Java Web Application Server Monitor

This chapter includes the main concepts, tasks, and reference information for the SAP Java Web Application Server monitor.

### **This chapter includes:**

#### **Concepts**

- ▶ SAP Java Web Application Server Monitor Overview on page 808

#### **Tasks**

- ▶ Configure the SAP Java Web Application Server Monitoring Environment on page 809

#### **Reference**

- ▶ SAP Java Web Application Server Monitor Settings on page 811

## SAP Java Web Application Server Monitor Overview

Use the SiteScope SAP Java Web Application Server monitor to monitor the availability and server statistics for SAP Java Web Application Server cluster. A Java cluster consists of one instance of Dispatcher per host, and one or more Servers. The monitor displays a counter tree for each dispatcher and server in the cluster. The SiteScope SAP Java Web Application Server monitor supports Web Application Server 6.40, Web Application Server 7.00, and SAP Enterprise Portal 5.0, 6.0 and 7.0.

---

### Note:

- ▶ The SAP Java Web Application monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a SAP Java Web Application server. For details on using the template, see “SAP Solution Templates” on page 1769.

---

To enable the SAP Java Web Application Server monitor, you must install the SAP JMX Connector. For details, see “Configure the SAP Java Web Application Server Monitoring Environment” on page 809.

For details on the user interface, see “SAP Java Web Application Server Monitor Settings” on page 811.



## Configure the SAP Java Web Application Server Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Download the SAP JMX Connector” on page 809
- “Enable the SAP Java Web Application Server Monitor” on page 810
- “Configure the Monitor Properties” on page 810

### 1 Download the SAP JMX Connector

The SAP JMX Connector (SAP JCo 2.0.6 and above) component must be downloaded and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

- a** To download SAP JMX Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>).

---

**Note:** You need a valid Service Marketplace login to access the SAP Web site

---

- b** Click **SAP Java Connector**, and then click **Tools and Services**.

## 2 Enable the SAP Java Web Application Server Monitor

The SAP Java Web Application Server monitor uses SAP JMX Connector libraries to connect to SAP J2EE cluster. A user must have the required license granted by SAP to receive and use these libraries.

- a** Rename the **logging.jar** file from the SAP Java Web Application server to **sap\_logging.jar** so as not to overwrite the SiteScope **logging.jar** file.
- b** Copy the following .jar files from the SAP Java Web Application server installation into the <SiteScope root directory>\WEB-INF\lib directory:
  - **admin.jar**
  - **com\_sap\_pj\_jmx.jar**
  - **exception.jar**
  - **sap\_logging.jar** (renamed from **logging.jar** in SAP library)
  - **jmx.jar**
- c** Restart SiteScope.

## 3 Configure the Monitor Properties

Complete the SAP Java Web Application monitor configuration. For details on the monitor settings, see “SAP Java Web Application Server Monitor Settings” on page 811.

## SAP Java Web Application Server Monitor Settings

<b>Description</b>	<p>The SAP Java Web Application Server monitor enables you to monitor the availability and server statistics for SAP Java Web Application server cluster.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the SAP Java Web Application Server Monitoring Environment” on page 809</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SAP Java Web Application Server Monitor Overview” on page 808</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## SAP Java Web Application Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Application server</b>	Enter the address of the SAP Java Web Application Server you want to monitor.
<b>Port</b>	Enter the number of the P4 port for the SAP Java Web Application Server you want to monitor. <b>Default value:</b> 50004
<b>Credentials</b>	Select the option for providing the user name and password to be used to access the SAP server. <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the SAP server in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor. These counters are received dynamically from the JMX. <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

# 74

---

## SAP Performance Monitor

This chapter includes the main concepts, tasks, and reference information for the SAP Performance monitor.

**This chapter includes:**

**Concepts**

- ▶ SAP Performance Monitor Overview on page 814

**Tasks**

- ▶ Configure the SAP Performance Monitoring Environment on page 815

**Reference**

- ▶ SAP Performance Monitor Settings on page 818

## SAP Performance Monitor Overview

Use the SAP Performance monitor to monitor the server and database performance data for SAP application servers R/3 4.6B, R/3 4.6C, R/3 4.7E, SAP ECC5 and SAP ECC6. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server and database loading for performance, availability, and capacity planning. Create a separate monitor instance for each SAP server in your environment.

---

### Note:

- ▶ The SAP Performance monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a SAP server. For details, see “SAP Solution Templates” on page 1769.

---

To enable the SAP Performance monitor, you must install the SAP Java Connector. For details, see “Configure the SAP Performance Monitoring Environment” on page 815.

This section also includes:

- ▶ “Setup Requirements and User Permissions” on page 815
- ▶ “Configuring the Monitor” on page 815

## Setup Requirements and User Permissions

A SAP user should have one or more of the profiles listed below assigned to it. Authorizations are collected in SAP profiles, and the following profiles include XMI authorization:

- S\_A.SYSTEM
- PD\_CHICAGO
- S\_WF\_RWTEST
- SAP\_ALL.

## Configuring the Monitor

For details on configuring the monitor, see “SAP Performance Monitor Settings” on page 818.

## Configure the SAP Performance Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Download the SAP Java Connector” on page 816
- “Enable the SAP Performance Monitor (on a Windows Environment)” on page 816
- “Enable the SAP Performance Monitor (on a UNIX Environment)” on page 817
- “Configure the Monitor Properties” on page 817

## 1 Download the SAP Java Connector

The SAP Java Connector (SAP JCo 2.0.6 and above) component must be downloaded and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

- a** To download SAP Java Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>).

---

**Note:** You need a valid Service Marketplace login to access the SAP Web site

---

- b** Click **SAP Java Connector**, and then click **Tools and Services**.

## 2 Enable the SAP Performance Monitor (on a Windows Environment)

The SAP Performance monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

- a** Download the following .jar file and .dll files from the SAP support Web site (<http://www.service.sap.com/connectors>):
  - **sapjco.jar**
  - **librfc32.dll**
  - **sapjcorfc.dll**
- b** Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.



- c Copy the two .dll files into the <SiteScope root directory>\bin directory.

---

**Note:** Check if the .dll files already exist in the <Windows installation directory>/system32 directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

---

- d Restart SiteScope.

### 3 Enable the SAP Performance Monitor (on a UNIX Environment)

The SAP Performance monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

- a Download the following .jar file and .so files from the SAP support Web site:
  - sapjco.jar
  - librfccm.so
  - libsapjcorfc.so
- b Copy the sapjco.jar file into the <SiteScope root directory>\WEB-INF\lib directory.
- c Copy the two .so files as follows:
  - For Sun installations, copy into the <SiteScope root directory>\java\lib\sparc directory.
  - For Linux installation, copy into the <SiteScope root directory>\java\lib\i386 directory.
- d Restart SiteScope.

### 4 Configure the Monitor Properties

Complete the SAP Performance monitor configuration. For details on the monitor settings, see “SAP Performance Monitor Settings” on page 818.

## SAP Performance Monitor Settings

<p><b>Description</b></p>	<p>The SAP Performance monitor enables you to monitor the availability and performance statistics of a SAP Application Server. The error and warning thresholds for the monitor can be set on SAP server and database performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “Configure the SAP Performance Monitoring Environment” on page 815</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “SAP Performance Monitor Overview” on page 814</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## SAP Performance Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Application server</b>	Enter the address of the SAP server you want to monitor.
<b>SAP client</b>	Enter the Client to use for connecting to SAP.
<b>System number</b>	Enter the System number for the SAP server.
<b>SAP router string</b>	<p>If your connection is being made through a router, enter a router address string, otherwise, leave it blank.</p> <p>You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select <b>Properties</b> to view the router address.</p>
<b>Credentials</b>	<p>Select the option for providing the user name and password to be used to access the SAP server.</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the SAP server in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>

GUI Element	Description
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>

# 75

---

## SAP Work Processes Monitor

This chapter includes the main concepts, tasks, and reference information for the SAP Work Processes monitor.

### **This chapter includes:**

#### Concepts

- ▶ SAP Work Processes Monitor Overview on page 822

#### Tasks

- ▶ Configure the SAP Work Processes Monitoring Environment on page 826

#### Reference

- ▶ SAP Work Processes Monitor Settings on page 829

## SAP Work Processes Monitor Overview

Use the SAP Work Processes monitor to monitor the effectiveness of your R/3 4.6B, R/3 4.6C, R/3 4.7E, SAP ECC5 and SAP ECC6 servers. The monitor provides statistical information on work process performance. This information enables you to estimate whether the SAP R/3 Server is efficiently using its resources.

---

**Note:** The SAP Work Processes monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

---

Using the SAP Work Processes monitor, you can also enable reporting of the host topology to Business Availability Center. If enabled, Business Availability Center automatically populates the CMDB with CIs based on the monitored hardware in SiteScope.

To enable the SAP Work Processes monitor, you must install the SAP Java Connector. For details, see “Configure the SAP Work Processes Monitoring Environment” on page 826.

This section contains the following topics:

- “Understanding the SAP Work Processes Monitor” on page 823
- “Setup Requirements and User Permissions” on page 823
- “SAP Work Processes Topology Settings” on page 824
- “Configuring the Monitor” on page 825

## Understanding the SAP Work Processes Monitor

A SAP work process is a program that runs the R/3 application tasks. Each work process acts as a specialized system service. In terms of the operating system, a group of parallel work processes makes up the R/3 runtime system.

Every work process specializes in a particular task type: dialog, batch, update, enqueue, spool, message, or gateway. In client/server terms, a work process is a service, and the computing system running the particular service is known as a server. For example, if the system is providing only dialog services, this is a dialog server, although commonly referred to as an application server.

The dispatcher assigns tasks to the free work processes, making optimal use of system resources and balancing the system load. The dispatcher knows and distributes pending tasks according to the type of the defined processes. The difference among the various work processes affects only those tasks or special services that have been assigned to the work processes through the dispatching strategy.

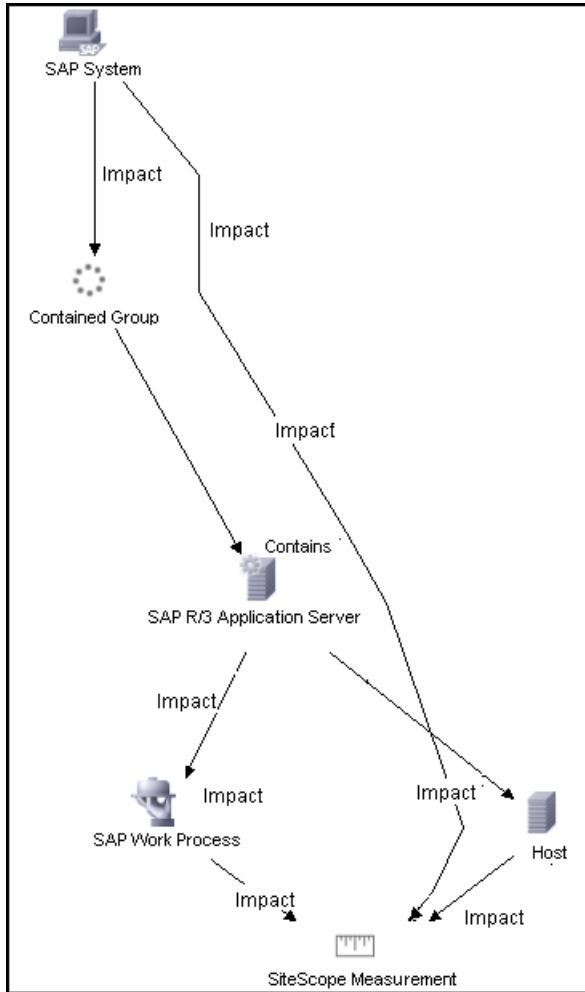
## Setup Requirements and User Permissions

A SAP user should have one or more of the profiles listed below assigned to it. Authorizations are collected in SAP profiles, and the following profiles include XMI authorization:

- S\_A.SYSTEM
- PD\_CHICAGO
- S\_WF\_RWTEST
- SAP\_ALL.

## SAP Work Processes Topology Settings

The SAP Work Processes monitor can identify the work processes of the server being monitored. If **Include topology data when reporting to BAC** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.





The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the Universal CMDB as SiteScope Measurement Groups and SiteScope Measurement CIs.

---

**Note:** This direct integration between SiteScope and Business Availability Center is available only when the Business Availability Center for SAP Applications license is installed.

---

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160 in the HP Business Availability Center Documentation Library.

For information about the SAP topology, see “SAP Systems View” in *Solutions and Integrations* in the HP Business Availability Center Documentation Library.

### **Configuring the Monitor**

For task details, see “Configure the SAP Work Processes Monitoring Environment” on page 826.

For user interface details, see “SAP Work Processes Monitor Settings” on page 829.

## **Configure the SAP Work Processes Monitoring Environment**

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- ▶ “Download the SAP Java Connector” on page 826
- ▶ “Enable the SAP Work Processes Monitor (on a Windows Environment)” on page 827
- ▶ “Enable the SAP Work Processes Monitor (on a UNIX Environment)” on page 828
- ▶ “Configure the Monitor Properties” on page 828

### **1 Download the SAP Java Connector**

The SAP Java Connector (SAP JCo 2.0.6 and above) component must be downloaded and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

- a** To download SAP Java Connector, go to the SAP Software Distribution Web site (<http://www.service.sap.com/connectors>).

---

**Note:** You need a valid Service Marketplace login to access the SAP Web site

---

- b** Click **SAP Java Connector**, and then click **Tools and Services**.

## 2 Enable the SAP Work Processes Monitor (on a Windows Environment)

The SAP Work Processes monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

- a** Download the following .jar file and .dll files from the SAP support Web site (<http://www.service.sap.com/connectors>):
  - **sapjco.jar**
  - **librfc32.dll**
  - **sapjcorfc.dll**
- b** Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.
- c** Copy the two .dll files into the **<SiteScope root directory>\bin** directory.

---

**Note:** Check if the .dll files already exist in the **<Windows installation directory>/system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

---

- d** Restart SiteScope.

### 3 Enable the SAP Work Processes Monitor (on a UNIX Environment)

The SAP Work Processes monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the required license granted by SAP to receive and use these libraries.

- a Download the following .jar file and .so files from the SAP support Web site:
  - **sapjco.jar**
  - **librfccm.so**
  - **libsapjcorfc.so**
- b Copy the **sapjco.jar** file into the **<SiteScope root directory>\WEB-INF\lib** directory.
- c Copy the two .so files as follows:
  - For Sun installations, copy into the **<SiteScope root directory>\java\lib\sparc** directory.
  - For Linux installation, copy into the **<SiteScope root directory>\java\lib\i386** directory.
- d Restart SiteScope.

### 4 Configure the Monitor Properties

Complete the SAP Work Processes monitor configuration. For details on the monitor settings, see “SAP Work Processes Monitor Settings” on page 829.

## SAP Work Processes Monitor Settings

<p><b>Description</b></p>	<p>The SAP Work Processes monitor enables you to monitor the effectiveness of your SAP R/3 server configurations. The monitor provides statistical information on work process performance to estimate whether the SAP R/3 Server is efficiently using its resources.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “Configure the SAP Work Processes Monitoring Environment” on page 826</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “SAP Work Processes Monitor Overview” on page 822</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## SAP Work Processes Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Application server</b>	Enter the address of the SAP server you want to monitor.
<b>SAP client</b>	Enter the Client to use for connecting to SAP.
<b>System number</b>	Enter the System number for the SAP server.
<b>SAP router string</b>	<p>If your connection is being made through a router, enter a router address string, otherwise, leave it blank.</p> <p>You can find the router address using the SAP Logon tool from the SAP Client software. Open the Logon console, select the server you want to monitor and then select <b>Properties</b> to view the router address.</p>
<b>Credentials</b>	<p>Select the option for providing the user name and password to be used to access the SAP server.</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the SAP server in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>

GUI Element	Description
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.  <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.





# 76

---

## Script Monitor

This chapter includes the main concepts, tasks, and reference information for the Script monitor.

### **This chapter includes:**

#### Concepts

- ▶ Script Monitor Overview on page 833

#### Tasks

- ▶ Set a Timeout Value for Script Monitor Instances on page 839

#### Reference

- ▶ Script Monitor Settings on page 840

### **Script Monitor Overview**

The Script monitor can be used to run shell commands or other scripts on the machine where SiteScope is running or it can run a script that is stored on a remote machine.

One of the primary reasons for using the Script monitor is to integrate into SiteScope an existing script that you use to do a particular system management function. For example, if you have a script that runs a diagnostic on an application and returns a 0 reading if everything is working, you could create a Script monitor that runs this script and recognizes any exit value other than 0 as an error. Then you could create an alert which would email or page you in the event that this monitor was in error.

The Script monitor supports monitoring remote servers running on HP NonStop operating systems.

---

**Note:** Symbolic links are now supported when executing scripts on remote UNIX servers. This support is enabled by setting the property `_scriptMonitorAllowSymbolicLink` to **true** (false by default) in the `master.config` file. When enabled, the symbolic link appears in the list of available scripts when configuring a Script monitor to monitor a UNIX remote.

---

This section contains the following topics:

- “Script Options” on page 835
- “Status” on page 836
- “Caching Script Output” on page 837
- “Setting a Timeout Value for Script Execution” on page 837
- “Running Different Types of Scripts” on page 838
- “Configuring the Monitor” on page 838

## Script Options

The following is an overview of the possible script execution options and requirements for the SiteScope Script monitor:

Script Option	Description
Local Script	A file stored and run on the SiteScope machine. The file should be stored in the <SiteScope root directory>\scripts directory.
Remote Script	<p>A remote script file (UNIX and Windows-Windows SSH only) in a scripts subdirectory in the home directory of the account SiteScope uses to access the remote server. For example, home/sitescope/scripts.</p> <p><b>Note:</b> Only executable script files are displayed.</p> <p>The remote scripts must include an echo construct to echo script results and exit codes back to SiteScope (see the Return Status Example section below).</p> <p>The monitor may fail if the required exit code is not echoed back to SiteScope.</p> <p>When running a script on a remote Windows server using SSH, you must include an "end script" string at the end of the script to avoid a timeout error. For example:</p> <pre>@echo off time echo end script</pre>
Remote Command	A script file containing a single command stored locally in the <SiteScope root directory>\scripts.remote directory. This script file is used to run a command on a remote server. The command may be used to run a remote script file that performs multiple functions.

---

**Note:** For SiteScope on Linux, the script itself must have a shell invocation line as the very first line of the script. This applies to scripts that you are trying to run locally on the SiteScope machine. For example, the first line of the script should include something like `#!/bin/sh` or `#!/usr/local/bin/perl`. If the shell invocation line is not found then the `exec()` call returns with a `-1` exit status. This is a limitation of the Java Runtime in JRE prior to release 1.4. This has been fixed in the 1.4 JRE from Sun which is shipped with SiteScope version 7.8 and later.

---

Scheduling Script monitors is dependent on the script that you want SiteScope to run. You can use the scheduling option to have SiteScope run scripts at different intervals throughout the week.

## **Status**

Each time the Script monitor runs, it returns a status and writes it into the monitoring log file. It also reports a command result, a value, and the time it took to run the command.

The command result is the exit value returned by running the command. This works for local UNIX scripts, but does not work for remote UNIX scripts, or Win NT batch files. Win NT batch file (\*.bat) exit codes are not passed out of the command interpreter, and remote UNIX script exit codes are not passed back through the remote connection. See the example below for a way to receive information from the script.

## Caching Script Output

The Script monitor includes an optional function that can be used to cache the output of a script execution. The cached output is useful in you want to have multiple script monitors check and alert on different parts of the output of a script, or reduce network traffic and server load by minimizing the number of times a script is run.

You can enable script output caching by entering a time value (in seconds) greater than zero in the **Cache life (seconds)** setting in the Monitor Settings section. To configure multiple Script monitors to use the data in the cache, each monitor instance must be:

- Configured to use the same remote Server profile.
- Configured to use the same Script file.
- Have a **Cache life (seconds)** value greater than zero.

The **Cache life (seconds)** value entered for each monitor should approach, but not exceed, the equivalent of the value selected for the **Frequency** setting for that monitor. For example, if the **Frequency** setting is 10 minutes, the **Cache life (seconds)** value can be set to a value of 590 because 10 minutes is equivalent to 600 seconds and 590 is less than 600. Any monitor that detects the end of its Cache Life runs the script again and refreshes the cache.

## Setting a Timeout Value for Script Execution

You can set a timeout value for the Script monitor for SiteScope running on Windows. The timeout value is the total time, in seconds, that SiteScope should wait for a successful run of the script. You can use this option to have SiteScope run the monitor but kill the script execution if a script exit code is not detected within the timeout period.

The requirements and limitations of this option are:

- It is only available with SiteScope for Windows.
- It can only be used with scripts stored and run on the local SiteScope server (that is, where the **Server** setting for the Script monitor is this server or localhost).

- The timeout setting value is expressed in seconds.
- It only applies to Script Monitors.

For details on how to set a timeout value for script execution, see “Script Monitor Settings” on page 840.

## Running Different Types of Scripts

You can run non-batch scripts, for example VBScript or Perl scripts, without wrapping them into a batch file (in versions of SiteScope earlier than 9.50, this was not possible).

---

**Note:** This is supported only on Windows machines where SiteScope Server is the target of the Script monitor.

---

- You can see scripts with any extensions that you specify in the `_scriptExtensions` property of the **master.config** file. For example, to see **.pl**, **.py**, or **.php** scripts, use the following format:  
`_scriptMonitorExtensions=.pl;.py;.php`
- You can run script interpreters with script extensions by specifying the `_scriptInterpreters` property of the **master.config** file as follows:  
`_scriptInterpreters=pl=c:/perl/perl.exe;py=c:/python/python.exe;php=c:/php/php.exe`

## Configuring the Monitor

For details on configuring the monitor, see “Script Monitor Settings” on page 840.

## Set a Timeout Value for Script Monitor Instances

Two methods exist for applying a timeout setting to Script monitors. One applies the setting as a property to an individual monitor. The second method adds the setting to groups, subgroups, or the entire SiteScope installation.

### To set a Timeout Value for individual script monitor instances:

- 1 Stop the SiteScope service.
- 2 Using a text editor, open the SiteScope group file containing the monitor frame for the Script monitor to which you want to apply the timeout setting.
- 3 Inside the Script monitor frame (delimited by the # sign), insert a line and add the timeout setting as `_timeout=time` where `time` is replaced with the time in seconds.
- 4 Save the group file.

---

**Note:** Do not add blank lines, leading or trailing spaces to any record in the group file.

---

- 5 Restart the SiteScope service.

### To set a Timeout Value for multiple script monitor instances:

- 1 Stop the SiteScope service.
- 2 Using a text editor, open the SiteScope group file containing one or more Script monitors to which you want to apply the timeout setting. Alternately, you can add the setting to the `SiteScope/groups/master.config` file.
- 3 Inside the group file frame at the top of the file before the first # symbol, insert a line and add the timeout setting as `_scriptMonitorTimeout=time` where `time` is replaced with the time in seconds.

- 4 Save the group file.

---

**Note:** Do not add blank lines, leading or trailing spaces to any record in the group file or **master.config** file.

---

- 5 Restart the SiteScope service.

## Script Monitor Settings

<p><b>Description</b></p>	<p>The Script monitor runs an external command and reports the result. It is one way to integrate existing system management scripts into the SiteScope environment. The Script monitor can be tailored to run scripts at regular intervals. In addition to reporting the command result, the Script monitor can also parse and report a specific value from the command output.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor supports monitoring remote servers running on HP NonStop operating systems.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying a Script monitor from a template, the case of the remote script name must match that of the script in the scripts subdirectory. Otherwise, the selected script is shown as 'none'.</li> </ul>



<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Set a Timeout Value for Script Monitor Instances” on page 839</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Script Monitor Overview” on page 833</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Script Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the script you want to run is stored. Select a server from the server list (only those Windows and UNIX remote servers configured in SiteScope via SSH are displayed).</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>

GUI Element	Description
<p><b>Script</b></p>	<p>Select the script to run. Only scripts placed into the <b>&lt;SiteScope root directory&gt;\scripts</b> directory may be used. In that directory, there are several examples scripts with comments describing each one.</p> <p>If you choose USE COMMAND, you must also specify a USE COMMAND script file name in the <b>Remote script command file</b> field below. SiteScope sends the command or commands found in the USE COMMAND script file to be run as a command line on the remote UNIX Machine. Script files for the USE COMMAND option must be created in the <b>&lt;SiteScope root directory&gt;\scripts.remote</b> directory.</p> <p><b>Example:</b> Create a file named <b>test.sh</b> and save it in the <b>&lt;SiteScope root directory&gt;\scripts.remote</b> directory. Edit <b>test.sh</b> to include the command syntax <code>ps -ef;echo "all done"</code> as the content of the file. Then create a Script monitor with the USE COMMAND option selected, select a remote UNIX machine, and select <b>test.sh</b> as the USE COMMAND script to run.</p> <p><b>Note:</b> The <b>diskSpace.bat</b> script accepts only two required parameters: host name and physical drive name. Because the connection to the remote host is made using the current SiteScope account, you can only use this script if SiteScope can access this account. If the specified account does not have the privileges to access the remote host, we recommend that you use the Disk Space monitor instead.</p>
<p><b>Parameters</b></p>	<p>Use to specify any additional parameters to pass to the script. Optionally, you can use a regular expression or one of SiteScope's date variables to insert date and time into the parameters box.</p> <p><b>Example:</b> <code>s/\$month\$ \$day\$ \$year\$/</code> passes the current month, day and year to the script.</p> <p><b>Syntax exceptions:</b> SiteScope cannot pass the following characters to scripts: ` ; &amp;   &lt; &gt;</p>

GUI Element	Description
<b>Output encoding</b>	<p>If the command output uses an encoding that is different than the encoding used on the server where SiteScope is running, select the code page or encoding to use. This enables SiteScope to match and display the encoded file content correctly.</p> <p><b>Default value:</b> windows-1252</p>
<b>Match value labels</b>	<p>Enter labels for the matched values found in the script output. The matched value labels are used as variables to access retained values from the match expression for use with the monitor threshold settings. These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.</p> <p><b>Example:</b> Enter Copyright_start, Copyright_end to represent the copyright date range used in the <b>Match expression</b> field. After the monitor runs, these labels are displayed in the Condition list in Threshold Settings, enabling you to set status threshold settings (Error if, Warning if, and Good if) for the matched value.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ Separate multiple labels with a comma (,).</li> <li>➤ You can set up to 10 labels.</li> </ul>

GUI Element	Description
<p><b>Match expression</b></p>	<p>To retrieve a value from the script output, enter a regular expression here. For example, the expression: <code>/(\d+)/</code> matches one or more digits returned by the script. Use parentheses to allow the monitor to retrieve these values as counters.</p> <p>By using the labels in <b>Match value labels</b>, these counters can be automatically assigned with a customized name and you can define thresholds for them. The retrieved value can be used to set the error or warning status of the monitor and to trigger alerts. SiteScope checks up to four values returned.</p> <p><b>Example:</b>  <code>/([UDTCP]{3,4})s*(\w\d\W]{5,35}\:d+)s*(\w\d\W]{5,35}\:d+)\s*([A-Z]{5,35})/s</code> could be used to match and retain values from the four columns of the following command output:</p> <pre>TCP planetcom:2664 COMSRVF01:2412 ESTABLISHED</pre> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ If this item is left blank, no value is retrieved from the script.</li> <li>▶ You can use up to 10 sets of parentheses to retain multiple values from the script output.</li> </ul>
<p><b>Open Tool</b></p>	<p>Click to open the Regular Expression Tool, which enables you to test a regular expression for content matching against a sample of the content you want to monitor. For details, see “Regular Expression Tool” on page 232.</p>

GUI Element	Description
<b>Remote script command file</b>	<p>If you have selected the USE COMMAND as the Script option and a remote machine as the Server, select the script file that contains the commands that SiteScope should send to the remote machine. You can save one or more commands in the text script file and save the file in the &lt;SiteScope root directory&gt;\<b>scripts.remote</b> directory. SiteScope opens this file and runs the command at the command line of the remote server chosen in the <b>Choose Server</b> option above. You can then use the Match Expression option to parse the output of the command and display valuable information.</p> <p>The USE COMMAND script can make use of positional parameters such as \$1, \$2 (or alternatively %1, %2), and so on, inside the script. Enter the parameters you want SiteScope to pass to the script in the Parameters box provided above.</p> <p>You can use one or more commands per USE COMMAND script file.</p> <p><b>Default value:</b> none</p> <p><b>Syntax exception:</b> Do not include any carriage returns or any command that would normally discontinue script processing (for example, do not use the exit command).</p>
<b>Cache life (seconds)</b>	<p>Use this option only if you want to use multiple Script monitor instances to check or match on content returned by a single run of a script.</p> <ul style="list-style-type: none"> <li>▶ Enter a time value (in seconds) greater than zero to have SiteScope cache the output of the script execution. Each time the monitor is run, SiteScope checks if the cache life has expired. If it has not, then the monitor uses the cached script output data, otherwise the script is run again to update the cache and the monitor.</li> <li>▶ Enter a value of <b>0</b> (zero) to disable the cache function. This causes the monitor to run the script each time that it runs.</li> </ul> <p><b>Default value:</b> 0</p>

GUI Element	Description
<b>Measurement maximum (milliseconds)</b>	<p>Enter a maximum value, in milliseconds, for creating the gauge display.</p> <p><b>Example:</b> If the runtime of the script is 4 seconds, and this value is set to 8 seconds (8000 milliseconds), the gauge shows at 50%.</p> <p><b>Default value:</b> 0</p>

# 77

---

## Service Monitor

This chapter includes the main concepts and reference information for the Service monitor.

**This chapter includes:**

**Concepts**

- ▶ Service Monitor Overview on page 848

**Reference**

- ▶ Service Monitor Settings on page 850

## Service Monitor Overview

The Service monitor verifies that specific services or processes are listed as running, and optionally, it can also check to see how much CPU and memory (Page File Bytes) a service or process is using. If a service or process that should be running does not show up or if it is using too much memory, SiteScope can either alert you to the problem so that you can address it yourself, or it can run a script to automatically restart the service or process to help minimize the effect on other operations and downtime.

You should create a Service monitor for any service or process that should be running on a consistent basis. You can also create a Script Alert that restarts the service automatically if the service monitor in SiteScope cannot find it. The **restartService.bat** script, located in the `<SiteScope root directory>\scripts` directory, is a template that you can customize to create a script for SiteScope to run in the event your monitor fails. For details on using a Script Alert, see “Working with Script Alerts” on page 1977.

This section contains the following topics:

- “Status” on page 848
- “Scheduling the Monitor” on page 849
- “Configuring the Monitor” on page 849

### **Status**

Each time the Service monitor runs, it returns a reading and a status message and writes them in the monitoring log file.

The reading is the current value of the monitor. For this monitor, the possible readings are:

- Running
- Not found

The status is logged as either OK or error. An error status is returned if the service is not found.



## **Scheduling the Monitor**

The Service monitor does not put a heavy load on your server. For monitoring remote UNIX servers, SiteScope usually needs to open a telnet or SSH connection to the remote server. While the monitor actions generally do not load either server, managing a large number of remote connections can result in some performance problems. You probably want to monitor critical services and services that have a history of problems every five minutes or so. Less critical services and processes should be monitored less frequently.

## **Configuring the Monitor**

For details on configuring the monitor, see “Service Monitor Settings” on page 850.



## Service Monitor Settings

<p><b>Description</b></p>	<p>The Service monitor checks to see if a service (Windows environment) or a specific process (UNIX and Windows) is running. There are many services or processes that play an important role in the proper functioning of your server, including Web server, Mail, FTP, News, Gopher, and Telnet. Web environments which support e-commerce transactions may have other important processes that support data exchange.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ In Threshold Settings, the CPU and memory (Page File Bytes) measurements are relevant only for processes and not for system services. If the selected service is a process name, CPU and memory (Page File Bytes) measurements are in the drop-down list. If the selected service is a system service, such as Event Log, CPU and memory (Page File Bytes) measurements are not listed.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> <li>▶ The <b>Services Tool</b> is available when configuring this monitor to view services running on the server where SiteScope is installed (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see "Services Tool" on page 234.</li> </ul>

<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Service Monitor Overview” on page 848</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Service Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the service or process you want to monitor is running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. Remote servers that have been configured with the WMI method are also displayed in the server list. For details, see “Configure the WMI Service for Remote Monitoring” on page 1284.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>
<b>Service</b>	<p>Select the service (or process in UNIX) that you want to monitor from the services list.</p> <p>To monitor an NT process, select <b>(Using Process Name)</b> in the drop-down list and enter the name in the <b>Process name</b> box.</p> <p><b>Note:</b> The CPU and memory (Page File Bytes) counters are relevant for processes and not for services, and it is displayed only if the selected service is by process name.</p>
<b>Other service</b>	<p>Enter the name of the service you want to monitor if it is not listed in the services list.</p> <p><b>Note:</b> This field is available only when <b>Unknown</b> is selected in the <b>Service</b> box.</p>

GUI Element	Description
<b>Process name</b>	<p>(For Windows only) If you want to get information about the percentage of CPU and memory (Page File Bytes) being used by a specific process and/or the number of a specific type of process running, enter the name of the process here. Use a string or a regular expression.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ The name of the process must be as it appears in NT Task Manager.</li> <li>▶ This field is available only when <b>(using Process name)</b> is selected in the <b>Service</b> box.</li> </ul> <p><b>Example:</b> explorer.exe</p>
<b>Measure process memory use</b>	<p>(For UNIX only) Select this box if you want SiteScope to report the amount of virtual memory being used by a specific process.</p>



# 78

---

## Siebel Application Server Monitor

This chapter includes the main concepts and reference information for the Siebel Application Server monitor.

**This chapter includes:**

**Concepts**

- ▶ Siebel Application Server Monitor Overview on page 856

**Reference**

- ▶ Siebel Application Server Monitor Settings on page 861

## Siebel Application Server Monitor Overview

The Siebel Application Server monitor (previously known as the Siebel Server Manager monitor) uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel 7.03, 7.04, 7.5.3, 7.7, and 8.0 application servers.

---

**Note:**

- ▶ The Siebel Application Server monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a Siebel application server. For details, see “Siebel Solution Templates” on page 1777.

---

This section contains the following topics:

- ▶ “Setup Requirements and User Permissions” on page 857
- ▶ “Siebel Application Server Topology Settings” on page 859
- ▶ “Configuring the Monitor” on page 860



## Setup Requirements and User Permissions

The following are requirements for using the Siebel Application Server monitor:

- ▶ The Siebel Server Manager client must be installed only on the machine where SiteScope is running or that is accessible to the SiteScope. There are several options for how you can do this:
  - ▶ Copy the necessary client libraries from the Siebel server and install them on the machine where SiteScope is running (recommended option).
  - ▶ Enable the client on the Siebel server itself and create a remote server profile in SiteScope to access that server and the Siebel client on that server.
  - ▶ Install and enable the client on a third remote server and create a remote server profile in SiteScope to access that server and the Siebel client on that server. This option is applicable only for UNIX remotes.
  - ▶ For Windows networks, map the network drive where the Siebel client is installed to the SiteScope machine and use this in the Script Path.
- ▶ You must know the install path for the Server Manager client to be able to setup Siebel Server Manager monitors in SiteScope. If the client is installed on the machine where SiteScope is running, this is the path on that machine. If the client is installed on a remote machine, you must know the fully qualified path to the client executable relative to that machine (usually called **svrvmgr** or **svrvmgr.exe**).
- ▶ You must know the name or address of the Siebel Gateway server used by the Siebel applications you want to monitor. Ask your Siebel system administrator or consult the Siebel documentation for more information about the Gateway server name.
- ▶ You must know the name or address of the Siebel Enterprise server used by the Siebel applications you want to monitor. Ask your Siebel system administrator or consult the Siebel documentation for more information.
- ▶ You must know the user and password that Server Manager uses for logging into the Siebel server. This user must be granted Siebel Administrator responsibility on the Siebel server.

- ▶ For monitoring Siebel processes, SiteScope needs credentials/authorization to access the target Siebel machine. You may need to define a Remote host in SiteScope for the target Siebel machine, unless the SiteScope server is already implicitly authenticated by the Siebel machine.

---

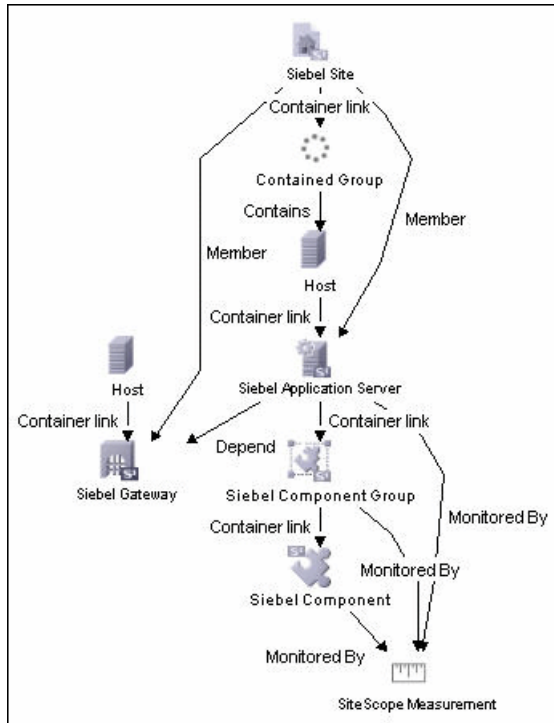
**Note:** Process monitoring remote Siebel machines incurs a noticeable delay (to get process metrics) hence the monitor runs slower than if the target Siebel machine is in close proximity to the SiteScope server. If your process counters are returning with no values during a run, it may be that the process metrics read operation is taking too long and SiteScope is timing out. In this case you may want to specify a required timeout value for perfex in the Infrastructure Settings Preferences page; for example, change the **Perfix timeout** value to 120 seconds. To access this setting, open the **Preferences** context, select **Infrastructure Settings Preferences**, and expand the **General Settings** section.

---

- ▶ **For SiteScope on Solaris/Linux.** You must make sure that the Siebel Server Manager Client's libraries are available to the Client. Set the `LD_LIBRARY_PATH` on that machine by using the Initialize Shell Environment field for the remote server configuration created in SiteScope. An example shell initialization command is `LD_LIBRARY_PATH=/var/siebel/client/lib;export LD_LIBRARY_PATH.`

## Siebel Application Server Topology Settings

The Siebel Application Server monitor can identify the topology of the Siebel Application Servers being monitored. If **Include topology data when reporting to BAC** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the Universal CMDB as SiteScope Measurement Groups and SiteScope Measurement CIs.

---

**Note:** This direct integration between SiteScope and Business Availability Center is available only when the Business Availability Center for Siebel Applications license is installed.

---

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160 in the HP Business Availability Center Documentation Library.

For information about the Siebel topology, see “Siebel Views” in *Solutions and Integrations* in the HP Business Availability Center Documentation Library.

### **Configuring the Monitor**

For details on configuring the monitor, see “Siebel Application Server Monitor Settings” on page 861.

## Siebel Application Server Monitor Settings

<p><b>Description</b></p>	<p>The Siebel Application Server monitor (previously know as the Siebel Server Manager monitor) uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel application servers.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b>, <b>Add Remote Server</b>, and <b>Add Credentials</b> buttons are not displayed.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Siebel Application Server Monitor Overview” on page 856</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Siebel Application Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Siebel host name</b>	<p>This box is required if you are doing either of the following:</p> <ul style="list-style-type: none"> <li>▶ <b>Doing process monitoring.</b> In this case you must define a Remote Definition to the target Siebel machine whose Siebel processes are to be monitored. Enter the <b>Host Server Name</b> of the Siebel Remote definition (not the <b>Title</b>). This is the <b>NT Server Address</b> box for NT remote servers or <b>Server Address</b> box for UNIX remote servers.</li> <li>▶ <b>Reporting monitor data to an installation of HP Business Availability Center.</b> In this case the value entered is used as a text identifier describing the target Siebel server that this monitor is monitoring. This text descriptor is used to identify the Siebel server when the monitor data is viewed in an HP Business Availability Center report. The box is optional only if the <b>Script Server</b> box is already specified to be the target Siebel server.</li> </ul>
<b>Application server</b>	Enter the Siebel server name or address.
<b>Gateway server</b>	Enter the Gateway server name or address.
<b>Enterprise server</b>	Enter the Enterprise server name or address.

GUI Element	Description
<b>Credentials</b>	<p>The Siebel Server Manager client requires a user name and password. Select the option to use for providing credentials:</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (selected by default). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>Script server</b>	<p>The remote Windows or UNIX machine where the Server Manager (srvrnmgr) script is installed. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p>The method of connection is either SSH or Telnet (but not Microsoft NetBios). For NetBios, choose this server and map the drive.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>
<b>Script path</b>	<p>The full path to the Siebel Server Manager executable directory relative to the machine chosen above.</p> <p><b>Example:</b> E:\sea704\client\BIN</p>
<b>Counters</b>	<p>The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p>



GUI Element	Description
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>
<b>Siebel tasks time window (minutes)</b>	<p>Specify a time window in which tasks are monitored on the Siebel application server. This setting applies only to the "No. of Tasks in XXX" counters. This value tells SiteScope to count tasks that have started within the last N minutes only. It can be used, for instance, to make SiteScope monitor only newly occurring tasks.</p> <p><b>Example:</b> If the task start time is within the time window (for example, 20 minutes), the task is monitored. The time window is calculated according to the formula: time window = (current time – property value).</p> <p>Enter 0 to monitor every task on the Siebel application server, regardless of its start time.</p> <p><b>Default value:</b> 60 minutes</p>



# 79

---

## Siebel Log File Monitor

This chapter includes the main concepts and reference information for the Siebel Log File monitor.

**This chapter includes:**

**Concepts**

- ▶ Siebel Log File Monitor Overview on page 868

**Reference**

- ▶ Siebel Log File Monitor Settings on page 869

## Siebel Log File Monitor Overview

Use the Siebel Log File monitor to automatically scan multiple log files for detailed data and error information. By having SiteScope scan the log files at set intervals, you can eliminate the need to scan the logs manually. In addition, you can be notified of warning conditions that you may have otherwise been unaware of until something more serious happened.

This monitor supports monitoring remote servers running on Siebel Application Server 7.03, 7.04, 7.5.3, 7.7, and 8.0.

---

**Note:** The Siebel Log File monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

---

Each time that SiteScope runs this monitor, it starts from the point in the file where it stopped reading last time it ran. This insures that you are only notified of new entries and speeds the rate at which the monitor runs. While this behavior can be overridden, we do not recommend it, and this should be done for troubleshooting purposes only.

You can schedule your Siebel Log File Monitors to run as often as every 15 seconds. However, depending on the size of the log files, the total number of monitors you have running, and whether the **Search from start** option is selected, the monitor may take a considerable amount of time to run.

For details on configuring the monitor, see “Siebel Log File Monitor Settings” on page 869.

## Siebel Log File Monitor Settings

<b>Description</b>	<p>The Siebel Log File monitor checks for log file entries added to a group of log files by looking for entries containing a specific event type or subtype.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Siebel Log File Monitor Overview” on page 868</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Siebel Log Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The Siebel server where the log files you want to monitor are running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b> To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</p>

GUI Element	Description
<b>Add Remote Server</b>	<p>Click to open the Add Remote Server dialog box. Select the type of remote you want to add (Windows or UNIX), and enter the configuration details.</p> <p>For details on the Microsoft Windows Remote Servers user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p>For details on the UNIX Remote Servers user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>
<b>Log file directory</b>	<p>Enter the path to the log directory you want to monitor.</p> <p>To monitor log files on a remote Windows NT/2000 server through NetBIOS, specify a UNC path to the remote directory.</p> <p><b>Example:</b> \\remoteserver\logFileDirectory</p> <p>If you are using SSH as a connection method to the remote NT server, you must select the <b>java library</b> and <b>ssh1</b> options for that remote.</p>
<b>File name (regular expr.)</b>	<p>Select the log files that you want to monitor. You must use a regular expression to specify multiple files, and the regular expression string must be enclosed in forward slashes (for example, /&lt;my reg exp&gt;/). The search is not recursive and only matches files listed within the log file directory.</p> <p><b>Note:</b> Selecting too many log files to monitor can significantly degrade SiteScope performance.</p>
<b>Severity</b>	<p>Select the severity level of entries to consider for matching. Entries that have the correct event type/subtype and have an equal or greater severity are matched. Those entries with lesser severity are ignored.</p> <p><b>Default value:</b> Fatal</p>
<b>Event type</b>	<p>Select the matching event type or subtype. The monitor reports how many log entries were found of the specified type.</p> <p><b>Default value:</b> GenericLog</p>

GUI Element	Description
<p><b>Log-entry content match</b></p>	<p>(Optional) You may specify an additional text string or regular expression to further narrow down the matched log entries. This match expression is run against the content returned from the initial <b>Severity</b> and <b>Event type</b> match.</p> <p>You use this option to find only those log entries with the selected severity an event type that meet this additional match criteria.</p>
<p><b>Search from start</b></p>	<p>Select to always check the contents of the whole file. If this option is not selected, SiteScope checks only newly-added records, starting at the time that the monitor was created (not when the file was created).</p> <p><b>Note:</b> Monitoring large numbers of log files with this option enabled may use large amounts of memory and CPU time. This can degrade SiteScope server performance.</p> <p><b>Default value:</b> Not selected</p>



# 80

---

## Siebel Web Server Monitor

This chapter includes the main concepts and reference information for the Siebel Web Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ Siebel Web Server Monitor Overview on page 873

#### Reference

- ▶ Siebel Web Server Monitor Settings on page 876

### **Siebel Web Server Monitor Overview**

Use the Siebel Web Server monitor to monitor statistical and operational information about a Siebel server by way of the Siebel Web server plug-in. You can use this monitor to watch Siebel server login session statistics and gauge the performance of the Siebel server Object Managers and database.

This monitor supports monitoring remote servers running on Siebel Application Server 7.03, 7.04, 7.5.3, 7.7, and 8.0.

**Note:**

- ▶ The Siebel Web Server monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
  - ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a Siebel Web server. For details, see “Siebel Solution Templates” on page 1777.
- 

This section contains the following topics:

- ▶ “Setup Requirements” on page 874
- ▶ “Siebel Web Server Topology Settings” on page 875
- ▶ “Configuring the Monitor” on page 876

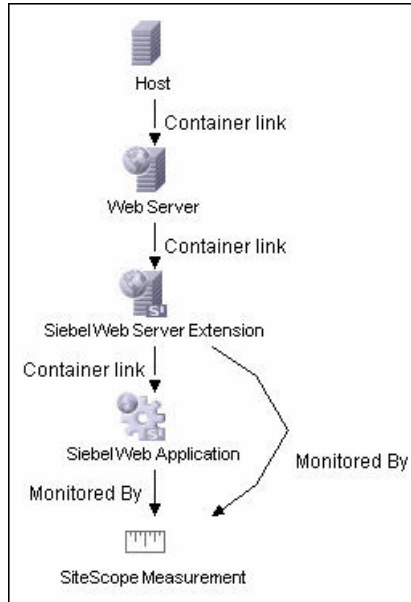
### **Setup Requirements**

The following are several key requirements for using the Siebel Web Server monitor:

- ▶ The Siebel Web server plug-in must be installed.
- ▶ The Siebel Web server plug-in should be configured to enable the display of the statistics you want to monitor. This may require that stats page sections be enabled by editing the **eapps.cfg** file for the Siebel server. Consult the Siebel documentation for more information.

## Siebel Web Server Topology Settings

The Siebel Web Server monitor can identify the topology of the Siebel Web Server being monitored. If **Include topology data when reporting to BAC** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the Universal CMDB as SiteScope Measurement Groups and SiteScope Measurement CIs.

---

**Note:** This direct integration between SiteScope and Business Availability Center is available only when the Business Availability Center for Siebel Applications license is installed.

---

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160.

For information about the Siebel topology, see “Siebel Views” in *Solutions and Integrations* in the HP Business Availability Center Documentation Library.

## Configuring the Monitor

For details on configuring the monitor, see “Siebel Web Server Monitor Settings” on page 876.

## Siebel Web Server Monitor Settings

<p><b>Description</b></p>	<p>The Siebel Web Server monitor enables you to use SiteScope to monitor statistical and operational information about a Siebel server by way of the Siebel Web server plug-in. You can use this monitor to watch Siebel server login session statistics and gauge the performance of the Siebel server Object Managers and database.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>

<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Siebel Web Server Monitor Overview” on page 873</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Siebel Web Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Basic Settings</b>	
<b>Application URL</b>	<p>Enter the URL of the Web plug-in server stats page for the application you want to monitor.</p> <p><b>Example:</b> <code>http://siebelsrv/service/_stats.swe</code></p> <p>If the Siebel Web server is configured to support verbose mode, you can also use <code>http://siebelsrv/service/_stats.swe?verbose=high</code> to include information on Locks and Current Operations Processing for the Siebel server.</p>
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>
<b>Connecton Settings</b> (These settings are optional, unless the server requires authentication)	
<b>Authorization user name</b>	Enter the user name to access the Web server stats page.

GUI Element	Description
<b>Authorization password</b>	Enter the password for accessing the Web server stats page.
<b>HTTP proxy</b>	If you are using a proxy to access the Siebel server, enter the proxy server and port to use. <b>Example:</b> proxy.SiteScope.com:8080
<b>Proxy server user name</b>	Enter the proxy user name if the proxy server requires authorization.
<b>Proxy server password</b>	Enter the proxy password if the proxy server requires authorization.  If access to the Siebel Web Server site is controlled by a centralized authorization and authentication access control system, the following fields are used to submit information to a HTML/CGI enabled authentication system.  You can determine if authentication is required by trying to access the Web plug-in server stats page using a Web browser outside of SiteScope. If an HTML-based authentication form opens before you see the Siebel service statistics page, you must use the following fields to access the Siebel Web server plug-in.
<b>HTML Form-Based Authentication</b> (These settings are optional, unless the server requires authentication)	
<b>HTML form-based authentication required</b>	Select this option to have SiteScope submit HTML form-based authentication when accessing the Siebel Web server plug-in.
<b>Authorization form name</b>	When using HTML Form-based Authentication, this is the identifier of the authentication form within the Web page. The identifier is a number representing the place or order of the forms on an HTML page.  <b>Example:</b> [1] is the first HTML <FORM> set, [2] is the second, and so on. The default is [1] because it assumes that the authentication information is entered into the first HTML <FORM> tag set on the page.

GUI Element	Description
<b>Authorization user name form field</b>	When using HTML Form-based Authentication, enter the user name that should be submitted to the access control system. This must be the user name that would be entered in the authentication form the same as if you were accessing the Siebel Web server plug-in manually using a Web browser.
<b>Authorization password form field</b>	Enter the password that should be submitted to the access control system. This must be the password that would be entered in the authentication form when accessing the Siebel Web server plug-in manually using a Web browser.
<b>Authorization form button</b>	<p>When using HTML Form-based Authentication, this is the identifier of the Submit button on the authentication form.</p> <p>The identifier is a number representing the place or order of the buttons on an HTML page.</p> <p><b>Example:</b> [1] is the first HTML &lt;INPUT TYPE=SUBMIT&gt; button, [2] is the second, and so on.</p> <p><b>Default value:</b> [1]</p>





# 81

---

## SNMP Monitor

This chapter includes the main concepts and reference information for the SNMP monitor.

**This chapter includes:**

**Concepts**

- ▶ SNMP Monitor Overview on page 882

**Reference**

- ▶ SNMP Monitor Settings on page 884

## **SNMP Monitor Overview**

Use the SNMP monitor to monitor devices that communicate with the SNMP protocol, such as firewalls, routers, and UPS's. Several operating systems suppliers also provide SNMP agents and Management Information Bases (MIBs) for accessing workstation or server performance metrics, interface statistics, and process tables by using SNMP. The monitor supports monitoring agents of SNMP versions 1.0, 2.0, and 3.0 MD5.

You can use the SNMP monitor to watch any values known by the SNMP agent running on a device, provided that you can supply an OID that maps to that value. If your router supports SNMP, for example, you could have SiteScope monitor for packet errors, bandwidth, or device status.

---

**Note:** To have SiteScope listen for SNMP traps from multiple devices, use the SNMP Trap monitor.

---

This section also includes:

- ▶ “Setup Requirements and User Permissions” on page 882
- ▶ “Configuring the Monitor” on page 883

### **Setup Requirements and User Permissions**

Requirements for using the SNMP monitor include:

- ▶ SNMP agents must be deployed and running on the servers and devices that you want to monitor.
- ▶ The SNMP agents must be supplied with the necessary Management Information Bases (MIBs) and configured to read those MIBs.
- ▶ If SNMP version 3 is used, a valid user name and password might be required to access the SNMP device.

- ▶ You must know the Object ID's (OIDs) of the parameters you want to monitor. In some cases, an equipment manufacturer may supply a list of OIDs that are available. Otherwise, you may need to locate a MIB browser utility to parse a MIB and extract the values of interest to you. If you want the monitor to get you the next OID of the OID you entered, you can enter the OID with a plus sign (+) at the end of the OID (for example, 1.3.6.1.2.1.4.3+). For each monitor run, the monitor retrieves the next OID value and not the OID that you entered. This may be helpful if you want to reach one of the SNMP table columns.

For information about monitoring SNMP systems, refer to the HP Software Self-solve knowledge base (<http://h20230.www2.hp.com/selfsolve/documents>). To enter the knowledge base, you must log in with your HP Passport ID.

## **Configuring the Monitor**

For details on configuring the monitor, see “SNMP Monitor Settings” on page 884.

 **SNMP Monitor Settings**

<b>Description</b>	<p>The SNMP monitor reads a value from an SNMP device. Many network devices support the SNMP protocol as a way of monitoring them. You must know the Object ID's for the device you want to monitor. These may be available in the product documentation or in the form of a MIB file. To have SiteScope listen for SNMP traps from multiple devices, use the SNMP monitor (see “SNMP Monitor Overview” on page 882).</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>SNMP Tool</b> is available when configuring this monitor to query a SNMP Management Information Base (MIB) and retrieve a set of OIDs (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “SNMP Tool” on page 241.</li> </ul>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SNMP Monitor Overview” on page 882</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## SNMP Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Basic SNMP Settings</b>	
<b>Host name</b>	Enter the host name or IP address of the SNMP device that you want to monitor (for example, demo.thiscompany.com). If your SNMP device is using a different port, add it to the host name using <b>:port</b> . <b>Example:</b> demo.SiteScope.com:170 (to use port 170)

GUI Element	Description
Object ID	<p>Select one of the following object ID settings:</p> <ul style="list-style-type: none"> <li>▶ <b>Commonly used values.</b> Select the Object ID mnemonic from the drop-down list. (This is the default option with <b>system.sysDescr</b> set as the default value.)</li> <li>▶ <b>Other values.</b> Enter the Object Identifier (OID) for the SNMP value you want to retrieve. The OID specifies which value should be retrieved from the device.</li> </ul> <p><b>Example:</b> 1.3.6.1.2.1.4.3</p> <p><b>Tip:</b> To troubleshooting basic connectivity to the device and to confirm that the SNMP agent is active, select the <b>system.sysDescr</b> object from the drop-down list if other objects cannot be found.</p> <p><b>Note:</b> SiteScope version 7.1 and later supports SNMP version 1 and version 2. To send a trap using snmpv2, you must select the version number in the SNMP Connection Settings.</p> <p>If you receive the error message <b>error - noSuchName</b>, it means SiteScope was able to contact the device but the OID given is not know by the device. You must provide an OID that is valid to the device to obtain a value.</p> <p>If you have a MIB file for the device you want to monitor, you can copy the *.mib (or *.my) file into the <b>&lt;SiteScope root directory&gt;\templates.mib</b> subdirectory and use the MIB Help utility to compile the MIB and browse the OIDs for the device. To use the MIB Helper tool, select <b>Tools &gt; MIB Browser</b> and enter the connection details. After copying a new MIB file to SiteScope, SiteScope must be restarted. Select the MIB file to browse using the drop-down list. Click the <b>browse</b> button to show the OIDs from the selected MIB file. A tree is displayed that represents the chosen MIB on the specified server. You can browse that tree to find the OID that you want to monitor.</p> <p><b>Note:</b> It is not necessary to browse a MIB file with the SiteScope Mib Helper to monitor a device. The MIB Helper is provided simply as a tool to help you discover OIDs available on a device, but it is not the only tool available. You can find other alternative tools on the Web (for example, MG-SOFT or iReasoning).</p>

GUI Element	Description
<b>Index</b>	<p>The index of the SNMP object. Values for an OID come as either scalar or indexed (array or table) values.</p> <ul style="list-style-type: none"> <li>➤ For a scalar OID, the index value must be set to 0.</li> <li>➤ For an indexed or table value, you must provide the index (a positive integer) to the element that contains the value you want. For example, OID 1.3.6.1.2.1.2.2.1.17 is an indexed value that contains four elements. To access this second element of this OID, enter an index of 2 in the <b>Index</b> text box. To access the fourth element, enter an Index value of 4.</li> </ul> <p>In some vendor specific MIB's, the indexed entries (often referred to in tables) can have compound index values. For example, the OID for the process entry table in a Sun Microsystems server MIB may be: .1.3.6.1.4.1.42.3.12.1.1. This indexed or table object may have up to eleven nodes with OIDs ranging from .1.3.6.1.4.1.42.3.12.1.1.1 to .1.3.6.1.4.1.42.3.12.1.1.11. Each of these nodes contains an indexed list of entries with index values that range from 0 to over 27300 where the Index value represents the process ID number used by the operating system (view examples using the ps -ef command in UNIX). In this example, the index values may not be consecutive from 0 to 27300.</p> <p><b>Default value:</b> 0</p>
<b>Community</b>	<p>Enter the Community string for the SNMP device.</p> <p>The Community string provides a level of security for a SNMP device. Most devices use <b>public</b> as a community string. However, the device you are going to monitor may require a different Community string to access it.</p> <p>If you try to monitor an SNMP agent through specific community, you must make sure that the SNMP agent is familiar with that community. For example, if you try to monitor a Windows 2003 server through public community, you must make sure that the SNMP agent has this community configured. Otherwise, the monitor cannot connect to the agent.</p> <p><b>Default value:</b> public</p> <p><b>Note:</b> The field is valid only for version 1 or 2 connections.</p>

GUI Element	Description
<b>SNMP Connection Settings</b>	
<b>Timeout (seconds)</b>	Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. <b>Default value:</b> 5 seconds
<b>Retry delay (seconds)</b>	Enter the number of seconds SiteScope should wait before retrying the request. It continues to retry at the interval specified here until the Timeout threshold is met. <b>Default value:</b> 1 second
<b>SNMP version</b>	Select the SNMP version used by the SNMP host you want to monitor. SiteScope supports SNMP version 1, version 2, and version 3. <b>Default value:</b> V1
<b>SNMP V3 user name</b>	If you are using SNMP version 3, enter the user name to be used for authentication. <b>Note:</b> SiteScope only supports MD5 authentication for SNMP V3.
<b>SNMP V3 password</b>	If you are using SNMP version 3, enter the password to be used for authentication for SNMP V3.
<b>SNMP Data Manipulation Settings</b>	
<b>Scaling</b>	If you choose a scaling option from the <b>Commonly used values</b> list, SiteScope divides the returned value by this factor before displaying it. Alternatively, you can specify a factor by which the value should be divided in the <b>Other values</b> box. <b>Default value:</b> No scaling
<b>Match content</b>	Use this item to match against an SNMP value, using a string or a regular expression or XML names. <b>Note:</b> You can click the <b>Open Tool</b> button to use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.



GUI Element	Description
<b>Units</b>	Enter an optional units string to append when displaying the value of this counter.
<b>Measurement label</b>	Enter an optional text string to describe the measurement being made by the monitor.
<b>Measure as delta</b>	Select this option to have SiteScope report the measurement as the difference between the current value and the previous value.
<b>Measure as rate per second</b>	Select this option to have SiteScope divide the measurement by the number of seconds since the last measurement.
<b>Percentage base</b>	Select a value to use for calculating the percentage base from the <b>Commonly used values</b> list or by typing a number or SNMP object ID in the <b>Other values</b> box. If entered, the measurement is divided by this value to calculate a percentage. If an object ID is entered, the <b>Index</b> value from the SNMP Monitor Settings pane is used.  <b>Default value:</b> No percentage base
<b>Measure base As Delta</b>	Select this option to have SiteScope calculate the Percentage Base as the difference between the current base and the previous base. Use this option when an SNMP object ID is used for Percentage Base and the object is not a fixed value.
<b>Gauge maximum</b>	Enter a maximum value for the Object ID. The maximum is calculated to create the gauge display (Optional).
<b>Secondary SNMP Settings</b> (To enable secondary object changes, you must add the property <code>_enableSecondSNMP=true</code> to the <code>master.config</code> file.)	
<b>Secondary object ID</b>	Select the object ID of the secondary SNMP object to be queried from the <b>Commonly used values</b> drop-down list, or enter the Object Identifier (OID) for the SNMP value you want to query in the <b>Other values</b> box.

GUI Element	Description
<b>Secondary match content</b>	<p>Use this item to set up a secondary SNMP index. Match this item against the main SNMP value using a string, regular expression (see “Using Regular Expressions” on page 261), or XML names (see “Monitoring XML Documents” on page 403).</p> <p><b>Example:</b> <code>/(\d)/</code> gets the first digit and uses it in the secondary index.</p>

# 82

---

## SNMP by MIB Monitor

This chapter includes the main concepts and reference information for the SNMP by MIB monitor.

### **This chapter includes:**

#### Concepts

- ▶ SNMP by MIB Monitor Overview on page 891

#### Tasks

- ▶ Configure the SNMP by MIB Monitoring Environment on page 893

#### Reference

- ▶ SNMP by MIB Monitor Settings on page 895

### **SNMP by MIB Monitor Overview**

The SNMP by MIB monitor gathers information from a source, organizes it into a browsable tree structure, and enables you to choose which items in the tree it should monitor. It works by connecting to the specified SNMP agent and performing a full traversal of the MIBs implemented by the agent. Thus, you do not need to know which objects are present on the agent in advance. The monitor supports agents of SNMP version 1, 2, and 3 MD5.

The MIB files in <SiteScope root directory>\**templates.mib** are then used to create a browsable tree that contains names and descriptions of the objects found during the traversal. An object may or may not be displayed with a textual name and description, depending on the MIBs available in **templates.mib**. SiteScope does not display objects for user selection when it has no knowledge of how to display those objects. For example, a plain OctetString may contain binary or ascii data, but SiteScope has no way to decode and display this data correctly without more information.

This section also includes:

- “Troubleshooting MIB Compilation” on page 892
- “Configuring the Monitor” on page 893

## Troubleshooting MIB Compilation

If MIBs are not listed in the **MIB file** drop-down box after adding MIB files to the **templates.mib** directory, perform the following MIB Compilation troubleshooting steps:

- 1** Open <SiteScope root directory>\**logs\RunMonitor.log** and look for MIB compilation error messages close to the time of your most recent restart. The error messages in the file contain descriptions of compilation errors encountered in each file, together with the line number that helps you identify the source of the errors.
- 2** Correct the errors found in **RunMonitor.log**. Usually, these errors can be fixed by one of the following:
  - Adding a MIB to **templates.mib** on which some of the new MIBs depend.
  - Removing a MIB from **templates.mib** which is duplicated or upgraded in the new MIBs.
  - Fixing broken comments in the new MIBs. Note that a comment is defined as follows: "ASN.1 comments commence with a pair of adjacent hyphens and end with the next pair of adjacent hyphens or at the end of the line, whichever occurs first." This means that a line containing only the string "----" is a syntax error, whereas the a line containing only the string "----" is a valid comment. Beware of lines containing only hyphens, as adding or subtracting a single hyphen from such lines may break compilation for that MIB.

- Fixing missing IMPORT statements. Some MIBs may neglect to import objects that they reference which are defined in other MIBs. You can also search in Web sites for the error that you get in **RunMonitor.log**. There is a lot of information about these errors on the Web.
- 3 After correcting the errors described in **RunMonitor.log**, restart SiteScope.
  - 4 Follow the procedures in “Add MIBs to the templates.mib Directory” on page 894 to verify that the new MIB files compiled correctly.

## Configuring the Monitor

For task details, see “Configure the SNMP by MIB Monitoring Environment” on page 893.

For user interface details, see “SNMP by MIB Monitor Settings” on page 895.

## Configure the SNMP by MIB Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Add MIBs to the templates.mib Directory” on page 894
- “Configure the Monitor Properties” on page 894

## 1 Add MIBs to the `templates.mib` Directory

You can add to the MIBs of which SiteScope is aware by putting new MIB files in the `templates.mib` directory.

---

**Note:** Since MIB files may depend on other MIB files, and because ASN.1 syntax is not always obeyed completely by vendors, you may encounter compilation errors with some MIBs.

---

- a** To check compilation of the new MIB, you can use the command line tool located in `<SiteScope root directory>\tools\SNMPMIBCompilation`. This tool enables you to check the new MIB compilation without having to restart SiteScope for every change you make in the MIB file. If the MIB is compiled using another tool (for example, MG-SOFT or iReasoning), you are not notified that the MIB file is compiled in SiteScope.
- b** Add new MIB files to the `templates.mib` directory. SiteScope only compiles MIBs in ASN.1 format which abide by the SMIV1 or SMIV2 standards.
- c** Restart SiteScope.
- d** Proceed to add a new SNMP by MIB monitor. Before adding the monitor, check that your new MIB files are listed in the **MIB file** drop-down box. If they are, then they were successfully compiled and you can use the SNMP by MIB monitor and the SNMP by MIB tool to browse devices that implement these MIBs.

If your newly added MIBs are not listed in the MIB File drop-down box, see “Troubleshooting MIB Compilation” on page 892.

## 2 Configure the Monitor Properties

Complete the SNMP by MIB monitor configuration. For details on the monitor settings, see “SNMP by MIB Monitor Settings” on page 895.

## SNMP by MIB Monitor Settings

<b>Description</b>	<p>The SNMP by MIB monitor enables you to monitor objects on any SNMP agent. The error and warning thresholds for the monitor can be set on one or more different objects.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ The <b>SNMP Browser Tool</b> is available when configuring this monitor to verify the connection properties of an SNMP agent and to gain more information about the MIBs which that agent implements (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “SNMP Browser Tool” on page 237.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the SNMP by MIB Monitoring Environment” on page 893</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SNMP by MIB Monitor Overview” on page 891</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## SNMP by MIB Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>SNMP Connection Settings</b>	
<b>Server</b>	Enter the name of the server you want to monitor.
<b>SNMP version</b>	Select the version of SNMP to use when connecting. SiteScope supports SNMP version 1, version 2, and version 3. Selecting V3 enables you to enter V3 settings in the SNMP V3 settings panel. <b>Default value:</b> V1
<b>Community</b>	Enter the community string. If you try to monitor SNMP agent through a specific community, you must make sure that the SNMP agent is familiar with that community. If you try to monitor Windows 2003 server through public community, you must make sure that the SNMP agent has this community configured. Otherwise, the monitor cannot connect to the agent. <b>Note:</b> This is valid only for version 1 or 2 connections. <b>Default value:</b> public
<b>Timeout (seconds)</b>	Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. <b>Default value:</b> 5 seconds
<b>Retries</b>	Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. <b>Default value:</b> 1
<b>Port</b>	Enter the port to use when requesting data from the SNMP agent. <b>Default value:</b> 161



GUI Element	Description
<b>Starting OID</b>	<p>Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered here.</p> <p><b>Default value:</b> 1</p> <p><b>Note:</b> You should edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value of 1 did not enable retrieving any counters, then you may have to enter a different value.</p>
<b>MIB File</b>	<p>Select the MIB file that contains the objects you want to monitor.</p> <p>If you select a specific MIB file, then only the objects described in that MIB file are displayed.</p> <p>If you select <b>All MIBs</b>, then all objects retrieved from the agent during the MIB traversal are displayed.</p> <p>If no MIB information is available for an object, it is still displayed but with no textual name or description.</p> <p>To make this monitor aware of new or additional MIBs, place new MIB files in the &lt;SiteScope root directory&gt;\<b>templates.mib</b> directory and restart SiteScope.</p> <p><b>Default value:</b> All MIBs</p>

GUI Element	Description
<b>Counter calculation mode</b>	<p>Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are:</p> <ul style="list-style-type: none"> <li>▶ <b>Calculate delta.</b> Calculates a simple delta of the current value from the previous value.</li> <li>▶ <b>Calculate rate</b> Calculates a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements.</li> <li>▶ <b>Do not calculate.</b> No calculation is performed.</li> </ul> <p><b>Note:</b> This option only applies to the aforementioned object types. An SNMP by MIB monitor that monitors Counter objects as well as DisplayString objects only performs this calculation on the Counter objects.</p> <p><b>Default value:</b> Do not calculate</p>
<p><b>V3 SNMP Settings</b> (This panel is enabled only if V3 is selected in the SNMP version field)</p>	
<b>SNMP V3 authentication type</b>	<p>Select the type of authentication to use for version 3 connections.</p> <p><b>Default value:</b> MD5</p>
<b>SNMP V3 user name</b>	<p>Enter the user name for version 3 connections.</p>
<b>SNMP V3 authentication password</b>	<p>Enter the authentication password to use for version 3 connections.</p>
<b>SNMP V3 privacy password</b>	<p>Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.</p>
<b>SNMP V3 context engine ID</b>	<p>Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.</p>
<b>SNMP V3 context name</b>	<p>Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.</p>

GUI Element	Description
<b>SNMP Counters</b>	
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ The counters displayed are those received during the timeout period, and may not include all the counters available on the server. Specifying a longer timeout in the Timeout (seconds) field in the SNMP Connection Settings panel may result in receiving more counters.</li> <li>▶ The total time for receiving the counters may be longer than the timeout specified, due to additional processing time not part of the request/response period.</li> <li>▶ Due to third-party counter restrictions, the total number of counters that can be monitored is limited to 32.</li> </ul> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>



# 83

---

## SNMP Trap Monitor

This chapter includes the main concepts and reference information for the SNMP Trap monitor.

### **This chapter includes:**

#### Concepts

- ▶ SNMP Trap Monitor Overview on page 901

#### Reference

- ▶ SNMP Trap Monitor Settings on page 903

### **SNMP Trap Monitor Overview**

---

**Note:** To have SiteScope query a specific device for a specific value, use the SNMP monitor.

---

Use the SNMP Trap monitor for automatically collecting SNMP Traps from other devices. With SiteScope doing this for you at set intervals, you can eliminate the need to check for the SNMP Traps manually. In addition, you can be notified of warning conditions that you may have otherwise been unaware of until something more serious happened. Each time that it runs this monitor, SiteScope checks traps that have been received since the last time it ran. The monitor supports monitoring traps of SNMP versions 1 and 2.

**Note:** The SNMP Trap monitor uses port 162 for receiving traps. If another application or process on the machine where SiteScope is running has bound this port, the monitor reports an **Address in use** error.

---

This section also includes:

- “Setup Requirements” on page 902
- “Configuring the Monitor” on page 902

### **Setup Requirements**

You must configure the network devices to send SNMP Traps to SiteScope. On Windows 2000 systems, this can be configured by using the **Administrative Tools > Services > SNMP Service > Properties > Traps** page. SNMP agents on UNIX platforms usually require that you edit the configuration files associated with the agent. For an example of working with other devices, see the instructions on the Cisco Web site for SNMP Traps and Cisco Devices.

### **Configuring the Monitor**

For details on configuring the monitor, see “SNMP Trap Monitor Settings” on page 903.

 **SNMP Trap Monitor Settings**

<b>Description</b>	<p>The SNMP Trap monitor checks for SNMP Traps received by SiteScope from other devices. The agents for the SNMP enabled devices must be configured to send traps to the SiteScope server.</p> <p><b>Note:</b> To have SiteScope query a specific device for a specific value, use the SNMP monitor, “SNMP Monitor Overview” on page 882.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>SNMP Trap Tool</b> is available when configuring this monitor to view SNMP Traps received by SiteScope's SNMP listener (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “SNMP Trap Tool” on page 243.</li> </ul>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SNMP Trap Monitor Overview” on page 901</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## SNMP Trap Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<p><b>Content match</b></p>	<p>Enter the text to look for in SNMP Traps. Regular expressions may also be used for pattern matching. By default, all SNMP traps received are matched.</p> <p>All SNMP Traps received by SiteScope are logged to <code>&lt;SiteScope root directory&gt;\logs\SNMPTrap.log</code> file.</p> <p><b>Example:</b> The following shows two traps received from one router and another trap received from a second router:</p> <pre>09:08:35 09/10/2001 from=router1/10.0.0.133 oid=.1.3.6.1.4.1.11.2.17.1 trap=link down specific=0 traptime=1000134506 community=public agent=router1/10.0.0.133 var1=The interface Serial1 is down</pre> <pre>09:08:45 09/10/2001 from=router1/10.0.0.133 oid=.1.3.6.1.4.1.11.2.17.1 trap=link up specific=0 traptime=1000134520 community=public agent=router1/10.0.0.133 var1=The interface Serial1 is up</pre> <pre>09:10:55 09/10/2001 from=router2/10.0.0.134 oid=.1.3.6.1.4.1.11.2.17.1 trap=enterprise specific specific=1000 traptime=1000134652 community=public agent=router2/10.0.0.134 var1=CPU usage is above 90%</pre> <p>The examples shown here may wrap across multiple lines to fit on this page. The actual traps are in a single extended line for each trap.</p>



GUI Element	Description
<b>Match value labels</b>	<p>Use this option to enter labels for the matched values found in the trap. The match value labels are used as variables to access retained values from the Content Match expression for use with the monitor threshold settings.</p> <p>You can set up to four labels. The labels are used to represent any retained values from the Content Match regular expression in the parameters available for the status threshold settings (Error if, Warning if, and Good if). These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.</p> <p><b>Note:</b> Separate multiple labels with a comma (,).</p>
<b>Run alerts</b>	<p>Select the method for running alerts:</p> <ul style="list-style-type: none"> <li>▶ If <b>For each SNMP Trap matched</b> is chosen, then the monitor triggers alerts for every matching entry found. When the SNMP Trap monitor is run for each SNMP Trap received, the monitor never reports a status of error or warning, regardless of the results of the content match or even if the target SNMP Trap is not found.</li> <li>▶ If <b>Once, after all SNMP Traps have been checked</b> is chosen, then the monitor counts up the number of matches and triggers alerts based on the <b>Error if</b> and <b>Warning if</b> thresholds defined for the monitor in the Threshold Settings section.</li> </ul> <p><b>Default value:</b> For each SNMP Trap matched</p>



# 84

---

## Solaris Zones Monitor

This chapter includes the main concepts, tasks, and reference information for the Solaris Zones monitor.

### **This chapter includes:**

#### Concepts

- ▶ Solaris Zones Monitor Overview on page 907

#### Tasks

- ▶ Analyze Solaris Zones Monitor Results - Use-Case Scenario on page 912

#### Reference

- ▶ Solaris Zones Monitor Settings on page 914

### **Solaris Zones Monitor Overview**

Use the Solaris Zones monitor to show statistics on the physical host, its zones, and their resource pools on Solaris servers. This monitor can help you recognize problems in the Solaris system, and isolate them in the zone or resource pool level. The Solaris Zones monitor supports monitoring machines that are running on Solaris 10 update 7 (5/09) operating systems.

The Solaris Zones monitor queries the list of UNIX servers currently configured in the UNIX Remote Servers container. To monitor a remote Solaris Zones server, you must define a UNIX Remote connection profile for the server before you can add a Solaris Zones monitor for that server. For details, see “Remote Servers Overview” on page 1276.

For details on how to analyze Solaris zones monitor results, see “Analyze Solaris Zones Monitor Results - Use-Case Scenario” on page 912.

This section contains the following topics:

- “Virtualization Support” on page 908
- “Solaris Zones Topology Settings” on page 909
- “Notes and Limitations” on page 909
- “Configuring the Monitor” on page 911

### **Virtualization Support**

A Solaris zone is a virtualized operating system environment created within a single instance of the Solaris Operating System. It provides the required isolation and security to run multiple applications of the same operating system on the same server.

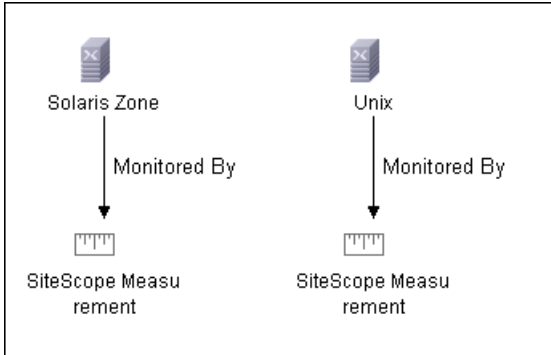
---

**Note:** Branded zones that are not of Solaris type are not supported.

---

## Solaris Zones Topology Settings

The Solaris Zones monitor can identify the topology of the Solaris system being monitored. If **Include topology data when reporting to BAC** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the Universal CMDB as SiteScope Measurement Groups CIs and the counters in it as SiteScope Measurement CIs. SiteScope Measurement CIs that refer to the physical host or global zone are linked to a UNIX host CI that represents the machine. SiteScope Measurement CIs that refer to a non-global zone are linked to a UNIX host CI that represents the zone. SiteScope can also report other measurements that are not connected to the host CIs. These can include pool measurements and counters in error.

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160 in the HP Business Availability Center Documentation Library.

### Notes and Limitations

- The monitor collects measurements for counters of running zones only. If a zone that was running is stopped or deleted, when the monitor next runs, the counters of this zone that were selected show n/a and the state string indicates that the zone is not running.

- ▶ When defining a Solaris remote server (by selecting Sun Solaris as the operating system), it does not necessarily mean that you can run special zone commands. To verify that zones are supported, run the **zoneadm** command, and check the output list contains the word **global** (this is the default zone that exists in any machine that supports zones). If it does not, the operating system does not support zones.
- ▶ A Solaris Zones monitor should be defined on a Solaris machine that supports Solaris Zones. The remote server should be defined on the machine itself (the global zone), and not on one of the machine's non-global zones. If the monitor is defined on a remote server that does not support zones, SiteScope identifies it by the output of the **zoneadm list** command. The output on operating systems that support zones always includes the global zone. If the global zone is not part of the command output (where the command is not supported), SiteScope displays the following error message: "The operating system does not support Solaris Zones".

---

**Note:** If the server goes down while running the **zoneadm** command, all the zones go down with it, and the server might be identified as a version that does not support zones.

---

- ▶ Some of the commands use **zlogin** to resolve the zone's data. Since this command can be used only by the global administrator operating in the global zone, you need to define your remote server with the global administrator user when selecting the zone's counters.
- ▶ While pool counters show all pools displayed by the **poolstat** command (including temporary pools), the **%usageOfPoolCpu** counter refers only to the pool defined for the zone in the **zonecfg** command, and does not include temporary dynamic pools. Where temporary pools are used, for example, by defining a **dedicated-cpu** resource for the zone, this counter does not reflect the real state.
- ▶ The **%usageOfPoolCpu** counter also takes account of the size of the pools, and assumes that pool size does not change during the monitor run.
- ▶ All counters that refer to pools, including all counters under the **Resource Pool** category and the **%usageOfPoolCpu** counter, show n/a if the pool facility is not active.

- ▶ Processes in the global zone can be bound to a pool used by another zone through a project. In this situation, the **%usageOfPoolCpu** counter (which takes into account only the pool configured to the zone in **zonecfg**), does not reflect the CPU usage out of all CPU power allocated to this zone's processes, since the potential CPU power available for the zone comes not only from its pool, but also from the other pools that its processes use.
- ▶ The **mbSize** zone counter has the same value in the SIZE and SWAP columns in the **prstat -Z** command output. In some versions of Solaris 10, the column is called SIZE and refers to the total address space size of all processes. In some later versions, the column is called SWAP and refers to the total swap (virtual memory) reserved by the zone's processes.
- ▶ If you create a Solaris Zones monitor and click **Save** (instead of **Verify & Save**), only a partial topology is reported to Business Availability Center. This topology includes the CIs of the measurements and measurement groups and the host CI of the machine itself (if some of its measurements were selected). The topology does not include the host CIs that represent the zones, since when saving only, no connection is made to the remote server to collect data that it has not already been collected (such as the zone's names in the network). These missing CIs are reported either:
  - ▶ If you make a change to the monitor, and click **Verify & Save**.
  - ▶ According to the **Topology resolving frequency (minutes)** value that is defined in **Preferences > Infrastructure Preferences > General Settings**. This is the amount of time, in minutes, to wait between checking the topology of the server being monitored (the default time is 120 minutes). If this time is exceeded during a monitor run, the monitor connects to the server to collect topology data (the zone's names in the network). If the data has changed or has not yet been reported, the monitor is put in the queue for reporting data. Since the queue is checked every hour, the monitor reports the topology again after a maximum of three hours since the time that the topology changed.

## Configuring the Monitor

For user-case scenario details, see “Analyze Solaris Zones Monitor Results - Use-Case Scenario” on page 912.

For user interface details, see “Solaris Zones Monitor Settings” on page 914.

## Analyze Solaris Zones Monitor Results - Use-Case Scenario

This section describes typical use-case scenarios in which the Solaris Zones monitor can be used to diagnose problems on the physical host, and in the zone and resource pool level.

This scenario includes the following steps:

- “Background” on page 912
- “High CPU Load in Zone1” on page 912
- “High CPU Load and Memory Consumption” on page 912
- “High CPU Load in a Resource Pool” on page 913

### **1 Background**

Bob, the SiteScope administrator for ABC Company, configures the Solaris Zones monitor to monitor the company’s Solaris system that comprises of four zones, two CPUs, and 4GB RAM.

### **2 High CPU Load in Zone1**

Bob notices that the physical host counters show CPU consumption of 51%, of which, according to zone1 counters, zone1 uses 50% of the machine's total CPU (no resource pools are used, so both CPUs can be used by each zone).

Now that Bob knows that the problem is with zone1, he can further investigate this zone.

### **3 High CPU Load and Memory Consumption**

The Solaris Zones monitor's physical host counters show that there is high CPU and memory consumption and excessive paging. After examining the counters results for each of the four zones, Bob discovers that zone2 consumes 2 GB of virtual memory.

Now that Bob knows that the problem is with zone2, he can further investigate this zone.



#### 4 High CPU Load in a Resource Pool

In this scenario, zone1 and zone2 use ResourcePool1 that contains one CPU, while all the other zones use the default pool that has the other CPU. Bob is alerted by the Solaris Zones monitor to the following:

- High CPU usage (100%) in ResourcePool1.
- The physical host counters in the Solaris Zones show CPU consumption of 51%.
- zone1 consumes 49-50% of the total machine CPU, while zone2 consumes only 0.4% (both of these zones use ResourcePool1).

Bob realizes that there is a problem with the existing resource allocation. Possible actions include:

- Assigning more CPU to zone1.
- Associating zone2 to the default pool to reduce the effect of poor performance from zone1.
- Stopping zone1 until the reason for the high CPU usage is found.

 **Solaris Zones Monitor Settings**

<b>Description</b>	<p>The Solaris Zones monitor enables you to monitor the physical host, its zones, and their resource pools on Solaris servers.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The monitor collects measurements for the zones that are in <b>Running</b> state only.</li> <li>▶ When configuring this monitor in template mode, you can use regular expressions to define counters.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Analyze Solaris Zones Monitor Results - Use-Case Scenario” on page 912</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Solaris Zones Monitor Overview” on page 907</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### Solaris Zones Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The Solaris server that you want to monitor. Select a server from the server list (only the UNIX remote servers that have been configured in SiteScope are displayed), or use the <b>Add Remote Servers</b> button to add a Solaris server.</p> <p><b>Note when working in template mode:</b></p> <ul style="list-style-type: none"> <li>▶ You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</li> <li>▶ There is a <b>Server to get measurements from</b> box with the list of UNIX servers from which you can select the server from which to get measurements.</li> </ul>
<b>Add Remote Server</b>	<p>Click to open the Add UNIX Remote Server dialog box and enter the configuration details. For details on the user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.</p>
<b>Counters</b>	<p>The server performance counters you want to check with this monitor. You can select counters on the physical host, its zones, and the resource pools used by the host. Use the <b>Get Counters</b> button to select counters.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p>



# 85

---

## SunONE Web Server Monitor

This chapter includes the main concepts and reference information for the SunONE Web Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ SunONE Web Server Monitor Overview on page 917

#### Reference

- ▶ SunONE Web Server Monitor Settings on page 919

### **SunONE Web Server Monitor Overview**

Use the SunONE Web Server monitor to monitor performance metrics reported in the stats-xml file of SunONE 6.x servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SunONE server you are running.

This section also includes:

- ▶ “Setup Requirements” on page 918
- ▶ “Configuring the Monitor” on page 918

## Setup Requirements

Before you can use the SunONE Web Server monitor, the **stats-xml** service option must be enabled on each Web server you want to monitor. This normally requires that you manually edit the **obj.conf** configuration file for each server instance. For iPlanet 6.0 servers, the entry has the following syntax:

```
<Object name="stats-xml">  
  ObjectType fn="force-type" type="text/xml"  
  Service fn="stats-xml"  
</Object>
```

Each server instance must be restarted for the changes to take effect.

## Configuring the Monitor

For details on configuring the monitor, see “SunONE Web Server Monitor Settings” on page 919.



## SunONE Web Server Monitor Settings

<p><b>Description</b></p>	<p>Enables you to monitor the availability of SunONE or iPlanet 6.x servers using the stats-xml performance metrics file (iwsstats.xml or nesstats.xml) facility.</p> <p>By providing the URL of this stats-xml file, SiteScope can parse and display all metrics reported in this file and enable you to choose those metrics you need to be monitored as counters. In addition, several derived counters are provided for your selection which measure percent utilization of certain system resources. Error and warning thresholds for the monitor can be set on one or more SunONE server performance statistics or HTTP response codes.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “SunONE Web Server Monitor Overview” on page 917</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## SunONE Web Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>Stats-XML URL</b>	Specify the URL to the stats-xml file on the SunONE server you want to monitor. This is usually in the form <code>http://server_id:port/stats-xml/&lt;stats-xml-file&gt;</code> where <code>&lt;stats-xml-file&gt;</code> is <code>nesstats.xml</code> or <code>iwsstats.xml</code> .
<b>Authorization user name</b>	Enter the user name of the SunONE server you want to monitor.
<b>Authorization password</b>	Enter the password of the SunONE server you want to monitor.
<b>HTTP proxy</b>	(Optional) A proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.
<b>Proxy server user name</b>	If the proxy server requires a name and password to access the server, enter the name here. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	If the proxy server requires a name and password to access the server, enter the password here.



GUI Element	Description
<b>Timeout (seconds)</b>	<p>The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 60 seconds</p> <p><b>Note:</b> Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with a timeout value of more than 60 seconds to enable the server time to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.</p>
<b>Counter Settings</b>	
<b>Counters</b>	<p>The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>



# 86

---

## Sybase Monitor

This chapter includes the main concepts and reference information for the Sybase monitor.

**This chapter includes:**

**Concepts**

- ▶ Sybase Monitor Overview on page 923

**Reference**

- ▶ Sybase Monitor Settings on page 925

### Sybase Monitor Overview

Use the Sybase monitor to monitor the server performance data for Sybase 11.0, 11.5, 11.92, and 12.x database servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Sybase server in your environment.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only.

---

This section also includes:

- ▶ “Setup Requirements” on page 924
- ▶ “Configuring the Monitor” on page 924

## Setup Requirements

- ▶ Before you can use the Sybase monitor, you have to configure the Sybase server environment. The Sybase monitor connects to the Sybase ASE server by using the Adaptive Server Enterprise Monitor Server and retrieves metrics from the server using Sybase-provided libraries. When connecting to the monitored server, you connect to the Adaptive Server Enterprise Monitor Server, not the Sybase server. The Adaptive Server Enterprise Monitor Server is an application that runs on the same machine as Sybase server and retrieves performance information from the Sybase server. The Adaptive Server Enterprise Monitor Server usually has the same server name as the Sybase server, but with the suffix `_ms`. For example, if the name of the Sybase database application server is `back-endddb`, the name of the Adaptive Server Enterprise Monitor Server for that server would be `back-endddb_ms`.
- ▶ You also have to install the Sybase Central client on the machine where SiteScope is running to connect to the Adaptive Server Enterprise Monitor Server. The version of the client software that you install must be at least as recent or more recent than the version of the server you are trying to monitor. For example, if you have Sybase version 11.0 servers, you must use the Sybase Central client version 11.0 or later. Copy the content of the `sql.ini` file located in `<System Root>\SYBASE\INI\` on the Sybase server into the `sql.ini` file on the SiteScope server. You can use the `dsedit` tool in the Sybase client console to test connectivity with the Adaptive Server Enterprise Monitor Server.

## Configuring the Monitor

For details on configuring the monitor, see “Sybase Monitor Settings” on page 925.

## Sybase Monitor Settings

<b>Description</b>	<p>The Sybase monitor enables you to monitor the availability and performance statistics of a Sybase Server. The error and warning thresholds for the monitor can be set on one or more Sybase server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Sybase Monitor Overview” on page 923</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### Sybase Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	Type the name of the server where the Sybase server you want to monitor is running. Usually it is the name of the server followed by <code>_MS</code> .
<b>User name</b>	Enter the user name to access the Sybase database.
<b>Password</b>	Enter the password of the user name to access the Sybase database.

GUI Element	Description
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.  <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

# 87

---

## Tuxedo Monitor

This chapter includes the main concepts and reference information for the Tuxedo monitor.

### **This chapter includes:**

#### Concepts

- ▶ Tuxedo Monitor Overview on page 927

#### Reference

- ▶ Tuxedo Monitor Settings on page 930

### **Tuxedo Monitor Overview**

Use the Tuxedo monitor to monitor the server performance data for BEA Tuxedo 6.5, 7.1, 8.0, 8.1, 9.0, and 9.1 servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Tuxedo server in your environment.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only. However, this monitor can monitor remote servers running on any platform/operating system.

---

This section also includes:

- “Setup Requirements” on page 928
- “Configuring the Monitor” on page 929

## Setup Requirements

The following are several key configuration requirements for using the Tuxedo monitor:

- If SiteScope is running as a machine in the same domain as the Tuxedo server then SiteScope can connect to the Tuxedo server as a native client. If SiteScope is outside the domain of the Tuxedo server, you must install, configure, and enable the Tuxedo Workstation component to enable SiteScope to make requests of the Tuxedo server.
- The client and server side workstation component software versions should be the same. Some versions of the client software can work with multiple versions of Tuxedo servers but support information is limited.
- If Tuxedo 7.1 or later is installed on both the server you want to monitor and the SiteScope server, more than one Tuxedo server can be monitored at a time. If Tuxedo 6.5 or earlier is used, only one Tuxedo server can be monitored at a time.
- If SiteScope is outside the domain of the Tuxedo server, the Tuxedo Workstation client software needs to be installed on the server where SiteScope is running. This is usually in a DLL called **libwsc.dll**. The address to the application server needs to be specified in the WSNADDR environment variable.



- On the server where the Tuxedo application server is running, set the **TUXDIR** variable to be the Tuxedo installation directory and add the **TUXEDO** bin directory to the **PATH** variable.

The following environment variables must be added to the SiteScope environment:

- **%TUXDIR%** should be set on the monitoring machine to the **<Tuxedo\_root\_folder>**
- **<Tuxedo\_root\_folder>\bin** should be added to **%PATH%** variable

---

**Note:** Any environment variables (for example, **TUXDIR**) should be defined as system variables, not user variables.

---

## Configuring the Monitor

For details on configuring the monitor, see “Tuxedo Monitor Settings” on page 930.

## Tuxedo Monitor Settings

<b>Description</b>	<p>The Tuxedo monitor enables you to monitor the availability of an BEA Tuxedo server. The error and warning thresholds for the monitor can be set on one or more Tuxedo monitor performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Tuxedo Monitor Overview” on page 927</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### Tuxedo Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Basic Tuxedo Settings</b>	
<b>Server</b>	<p>Enter the name or IP address of the server. The address should match that dedicated to the Tuxedo Workstation component (the WSL process).</p> <p>On UNIX servers, enter the full path of the applicable server.</p>

GUI Element	Description
<b>Port</b>	Enter the port number for the Tuxedo server. The port number should match the port dedicated to the Tuxedo Workstation component (the WSL process).
<b>User name</b>	Enter the user name if required to access the Tuxedo server.
<b>Password</b>	Enter the Password if required to access the Tuxedo server.
<b>Advanced Tuxedo Settings</b>	
<b>Client name</b>	Enter an optional client name for the Tuxedo server.
<b>Connection data</b>	Enter any extra or optional Connection Data to be used for connecting to the Tuxedo server. In some cases, this may be a hexadecimal number.
<b>Tuxedo Counters</b>	
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.  <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.



# 88

---

## UDDI Monitor

This chapter includes the main concepts and reference information for the UDDI monitor.

### **This chapter includes:**

#### Concepts

- ▶ UDDI Monitor Overview on page 933

#### Reference

- ▶ UDDI Monitor Settings on page 934

### **UDDI Monitor Overview**

Use the UDDI monitor to check the availability and round-trip response time of the UDDI 2.0 server. Each time that the monitor is run, SiteScope checks if the UDDI Server can find a business entity. The administrator of the UDDI server can limit or disable this monitor.

For details on configuring the monitor, see “UDDI Monitor Settings” on page 934.

## UDDI Monitor Settings

<b>Description</b>	<p>The UDDI monitor checks the availability and round-trip response time of the UDDI server.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.
<b>Included in Tasks</b>	"Deploy a Monitor – Workflow" on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ "UDDI Monitor Overview" on page 933</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 354.</li> </ul>

### UDDI Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Inquiry URL</b>	<p>Enter the UDDI server inquiry URL.</p> <p><b>Example:</b> <code>http://uddi.company.com/inquiry/</code></p>
<b>Business name</b>	<p>Enter the business entity to search for in the UDDI server.</p>
<b>Maximum number of businesses</b>	<p>The maximum allowed business entities to receive from the UDDI server (1–200).</p> <p><b>Default value:</b> 10</p>

# 89

---

## UNIX Resources Monitor

This chapter includes the main concepts and reference information for the UNIX Resources monitor.

### **This chapter includes:**

#### Concepts

- ▶ UNIX Resources Monitor Overview on page 935

#### Reference

- ▶ UNIX Resources Monitor Settings on page 937

### **UNIX Resources Monitor Overview**

Use the UNIX Resources monitor to monitor the server system statistics on UNIX servers. You can monitor multiple parameters or measurements with a single monitor instance. This enables you to monitor the remote server for loading, performance, and availability at a basic system level. Create a separate UNIX Resources monitor instance for each UNIX server in your environment.

The UNIX Resources monitor queries the list of UNIX servers currently configured in the UNIX Remote Servers container. To monitor a remote UNIX server, you must define a UNIX Remote connection profile for the server before you can add a UNIX Resources monitor for that server. For details, see “Remote Servers Overview” on page 1276.

This section contains the following topics:

- “Supported Versions” on page 936
- “Server-Centric Report” on page 936
- “Configuring the Monitor” on page 936

## Supported Versions

This monitor supports monitoring UNIX remote servers running on:

- Solaris 2.7, 2.8, 2.9, 5.10, 7, 8, 9, 10
- RedHat Linux 7.x, 8.x, 9.x, and Redhat Linux AS/ES Linux 3.x
- HP-UX 11iv1 (B.11.11) on HP 9000 series:
  - HP-UX B.11.11 U 9000/800 4030070275 unlimited-user license
  - HP-UX B.11.31 U ia64 4005705783 unlimited-user license
- AIX 5.2, 5.3

---

**Note:** The UNIX Resources monitor does not support monitoring remote servers running on HP NonStop operating systems. You should use the NonStop Resources Monitor instead.

---

## Server-Centric Report

You can create a Server-Centric report for the UNIX Server by clicking the server name in the Target column of the row corresponding to the UNIX Resources monitor in the Dashboard. For details, see “Server-Centric Report” on page 1881.

## Configuring the Monitor

For details on configuring the monitor, see “UNIX Resources Monitor Settings” on page 937.





## UNIX Resources Monitor Settings

<b>Description</b>	<p>The UNIX Resources monitor enables you to monitor multiple system statistics on a single UNIX system. The error and warning thresholds for the monitor can be set on one or more server system statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ When configuring this monitor in template mode, you can use regular expressions to define counters.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “UNIX Resources Monitor Overview” on page 935</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## UNIX Resources Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The UNIX server that you want to monitor. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed), or click the <b>Add Remote Servers</b> button to add a UNIX server.</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p>
<b>Server to get measurements from</b>	(Available in template mode only) Enter the name of any SiteScope remote server from which you want to get counters.
<b>Add Remote Server</b>	Click to open the Add UNIX Remote Server dialog box and enter the configuration details. For details on the user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.
<b>Available Counters</b>	<p>Displays the available measurements for this monitor.</p> <p>For each measurement, select the <b>Object, Instances and Counters</b> you want to check with the UNIX Resources monitor, and click the <b>Add Selected Counters</b>  button. The selected measurements are moved to the Selected Counters list.</p>

GUI Element	Description
<b>Selected Counters</b>	Displays the measurements currently selected for this monitor, and the total number of selected counters.  To remove measurements selected for monitoring, select the required measurements, and click the <b>Remove Selected Counters</b>  button. The measurements are moved to the Available Counters list.
<b>Enable Server-Centric Report</b>	Select to enable collecting data specifically for generating the Server-Centric report. The report displays various measurements for the server being monitored. For details, see “Generating a Server-Centric Report” on page 1881.



# 90

---

## URL Monitor

This chapter includes the main concepts, tasks, and reference information for the URL monitor.

### **This chapter includes:**

#### Concepts

- URL Monitor Overview on page 941

#### Tasks

- Configure the URL Monitoring Environment on page 946

#### Reference

- URL Monitor Settings on page 948

### **URL Monitor Overview**

The URL monitor is used to monitor a specified Web page to verify that it can be retrieved. The URL monitor supports monitoring HTTP versions 1.0 and 1.1. You can also use the URL monitor to do the following:

- Check secure pages using SSL, 128 bit SSL, and client certificates
- Check for specific content on the retrieved Web page
- Check the Web page for change
- Check for specific error messages
- Check the Web page for a value

- Retrieve detailed download information
- Check XML

When the URL monitor retrieves a Web page, it retrieves the page's contents. A successful page retrieval is an indication that your Web server is functioning properly. The URL monitor does not automatically retrieve any objects linked from the page, such as images or frames. You can, however, instruct SiteScope to retrieve the images on the page by selecting **Retrieve images** or **Retrieve frames** in the HTTP Settings pane.

In addition to retrieving specific Web pages, the URL monitor can verify that CGI scripts and back-end databases are functioning properly. You must input the complete URL used to retrieve data from your database or trigger one of your CGI scripts. The URL monitor verifies that the script generates a page and returns it to the user. For example, you can verify that your visitors are receiving a thank you page when they purchase something from your site. The URL monitor's string matching capability enables you to verify that the contents of the page are correct.

This section contains the following topics:

- “What to Monitor” on page 943
- “Status” on page 943
- “Scheduling the Monitor” on page 944
- “Setup Requirements and User Permissions” on page 944
- “SSL Connectivity” on page 945
- “Troubleshooting and Limitations” on page 945
- “Configuring the Monitor” on page 945

## What to Monitor

You can create URL monitors to watch pages that are critical to your Web site (such as your home page), pages that are generated dynamically, and pages that depend on other applications to work correctly (such as pages that utilize a back-end database). The goal is to monitor a sampling of every type of page you serve to check that things are working. There is no need to verify that every page of a particular type is working correctly.

When you choose which pages to monitor, select pages with the lowest overhead. For example, if you have several pages that are generated by another application, monitor the shortest one with the fewest graphics. This puts less load on your server while still providing you with the information you need about system availability.

## Status

Each time the URL monitor runs, it returns a reading and a status and writes it in the monitoring log file. It also writes in the log file the total time it takes to receive the designated document. This status value is also displayed in the SiteScope Monitor tables and is included as part of alert messages sent by using e-mail.

The status reading shows the most recent result for the monitor. This status value is displayed in the URL Group table within SiteScope. It is also recorded in the SiteScope log files, email alert messages, and can be transmitted as a pager alert. The possible status values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- document moved
- unauthorized
- forbidden

- not found
- proxy authentication required
- server error
- not implemented
- server busy

The status is logged as either good, warning, or error in the Dashboard. A warning status or error status is returned if the current value of the monitor is a condition that you have defined as other than OK.

### **Scheduling the Monitor**

Each URL monitor puts no more load on your server than someone accessing your site and retrieving a page, so in most cases you can schedule them as closely together as you want. Keep in mind that the length of time between each run of a monitor is equal to the amount of time that can elapse before you are notified of a possible problem.

A common strategy is to schedule monitors for very critical pages to run every 1 to 2 minutes, and then schedule monitors for less critical pages to run only every 10 minutes or so. Using this strategy, you are notified immediately if a critical page goes down or if the entire Web site goes down, but you do not have an excessive number of monitors running simultaneously.

### **Setup Requirements and User Permissions**

The user name and password specified in the **Credentials** section must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.



## SSL Connectivity

Web servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The `http://` prefix means that the server uses a non-encrypted connection. The `https://` prefix means that it is a secure, encrypted connection. Monitoring a Web server which uses an encrypted connection, requires either:

- ▶ Selecting the **Accept untrusted certificates for HTTPS** option in the Authentication Settings section of the Monitor Settings panel. For details, see “URL Monitor Settings” on page 948.
- ▶ Importing the server certificate. For details on how to perform this task, see “Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)” on page 946.

## Troubleshooting and Limitations

You can use the URL Sequence Tool to get on the spot data for the URL and to view the HTML received from the HTTP request.

## Configuring the Monitor

For task details, see “Configure the URL Monitoring Environment” on page 946.

For user interface details, see “URL Monitor Settings” on page 948.

## **Configure the URL Monitoring Environment**

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)” on page 946
- “Configure the Monitor Properties” on page 946

### **1 Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)**

If the Web server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate. Use one of the following methods for importing server certificates:

- Import the server certificates using SiteScope Certificate Management. For details, see “Import Server Certificates Using Certificate Management” on page 1537.
- Import the server certificates manually. For details, see “Import Server Certificates Manually” on page 947.

### **2 Configure the Monitor Properties**

Complete the URL monitor configuration. For details on the monitor settings, see “URL Monitor Settings” on page 948.

## Import Server Certificates Manually

Instead of using Certificate Management, you can import certificates manually using the keytool method, if preferred. Certificates imported this way can still be managed using Certificate Management. For details on Certificate Management, see “Certificate Management” on page 1535.

### To import server certificates manually:

- 1 Check the certificates already in the keystore, from the `<SiteScope root directory>\java\lib\security` directory, by entering:
 

```
../bin/keytool -list -keystore cacerts
```
- 2 Import the certificate, into `<SiteScope root directory>\java\lib\security`, by entering:

```
../bin/keytool -import -file myCert.cer -alias myalias -keystore cacerts
```

where `myCert.cer` is the certificate file name and `myalias` is the certificate alias.

Make sure that you specify a unique alias for every certificate you add. If you do not, the keytool uses an automatic alias and once you attempt to add more than one custom certificate, the new certificate overwrites the old and keeps the default alias.

The word `changeit` is the default password for the `cacerts` file.

---

**Note:** The default `cacerts` file is overwritten every time SiteScope is upgraded or re-installed. Therefore, you should create a copy of the `cacerts` file with a different name before SiteScope is upgraded or re-installed so that the file is not overwritten when new certificates are imported.

---

- 3 In SiteScope, select **Preferences > Certificate Management**, and click the **Reload Certificate List** button to reload the keystore certificates from the `cacerts` file. This enables you to manually reload keystore changes without having to restart SiteScope.



## URL Monitor Settings

<p><b>Description</b></p>	<p>Provides you with end-to-end verification that your Web server is running, serving pages correctly, and doing so in a timely manner. It tests end-to-end, so it is also able to determine whether back-end databases are available, verify the content of dynamically generated pages, check for changed content, and look for specific values from a page.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>➤ Monitors must be created in a group in the monitor tree.</li> <li>➤ While the <b>round trip time</b> performance counter is measured in milliseconds in the Threshold Settings, it is displayed in seconds in the Dashboard.</li> <li>➤ The <b>Get URL Tool</b> is available when configuring this monitor to request a URL from a server, print the returned data, and test network routing (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “URL Tool” on page 247.</li> </ul>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>➤ “Configure the URL Monitoring Environment” on page 946</li> <li>➤ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ “URL Monitor Overview” on page 941</li> <li>➤ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## URL Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Main Settings</b>	
<b>URL</b>	<p>Enter the URL that you want to monitor.</p> <p><b>Example:</b> http://demo.thiscompany.com</p> <p>For HTTPS monitoring (secure HTTP), if the URL starts with HTTPS, then a secure connection is made using SSL. SiteScope uses Java SSL libraries for HTTPS monitoring.</p> <p><b>Example:</b> https://www.thiscompany.com</p>
<b>Match content</b>	<p>Enter a string of text to match in the returned page or frameset.</p> <p>If the text is not contained in the page, the monitor displays the message content match error.</p> <p>HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for. This works for XML pages as well.</p> <p><b>Example:</b> &lt; B&gt; Hello&lt; /B&gt; World</p> <p>You can also perform a regular expression match by enclosing the string in forward slashes, with a letter i after the trailing slash indicating case-insensitive matching.</p> <p><b>Example:</b> /href=Doc\d+\.html/ or /href=doc\d+\.html/i</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ The search is case sensitive.</li> <li>➤ You can click the <b>Open Tool</b> button to use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</li> </ul>

GUI Element	Description
<p><b>Match content for error</b></p>	<p>Enter a string of text to check for in the returned page or frameset. If the text is contained in the page, the monitor indicates an error condition.</p> <p>HTML tags are part of a text document, so include them if they are part of the text for which you are searching.</p> <p><b>Example:</b>&lt; B&gt; Error &lt; /B&gt; Message</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash indicating case-insensitive matching.</p> <p><b>Example:</b> /href=Doc\d+\.html/ or /href=doc\d+\.html/i</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ The search is case sensitive.</li> <li>➤ You can click the <b>Open Tool</b> button to use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</li> </ul>
<p><b>Show detailed measurement</b></p>	<p>Select this box if you want SiteScope to record a detailed breakdown of the process times involved in retrieving the requested URL.</p> <p>These measurements include the following:</p> <ul style="list-style-type: none"> <li>➤ <b>DNS lookup time.</b> The time it takes to send a name resolution request to your DNS server until you get a reply.</li> <li>➤ <b>Connection time.</b> The time it takes to establish a TCP/IP/Socket connection to the Web server.</li> <li>➤ <b>Server response time.</b> The time after the request is sent until the first byte (rather first buffer full) of the page comes back.</li> <li>➤ <b>Download time.</b> The time it takes to download the entire page.</li> </ul>

GUI Element	Description
<b>Timeout (seconds)</b>	<p>The number of seconds that the URL monitor should wait for a page to complete downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status.</p> <p>If you have selected the <b>Retrieve images</b> or <b>Retrieve frames</b> option, SiteScope waits for these items to be retrieved before considering the page to be fully downloaded.</p> <p><b>Default value:</b> 60 seconds</p>
<b>Retries</b>	<p>Enter the number of times (between 0-10) that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request is a recoverable error.</p> <p><b>Default value:</b> 0</p>
<b>HTTP Settings</b>	
<b>Request headers</b>	<p>The header request lines sent by the HTTP client to the server. Headers should be linebreak separated. The standard list of HTTP1.1 request headers can be found in <a href="http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14">http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14</a>.</p> <p><b>Note:</b> Although this field is optional, some Web pages behave unexpectedly when the request header is missing (such as performing endless redirects, providing wrong content, and so forth).</p>
<b>URL content encoding</b>	<p>SiteScope retrieves the correct encoding from the server response. The default value appearing here should not be edited.</p> <p><b>Default value:</b> Retrieve encoding from server response</p>

GUI Element	Description
<b>POST data</b>	<p>If the URL is for a POST request, enter the post variables, one per line as name=value pairs.</p> <p>This option is used to verify that a form is working correctly by performing the same request that occurs when a user submits a form. See also the <b>Match content</b> item for a way to verify that the correct form response was received.</p> <p>If this item is blank, a GET request is performed.</p> <p>The POST data can be used to send cookie data. To send cookies with the request, use the format <b>Set-cookie:</b> cookieName=cookieValue.</p> <p>To change the content type of a post, use the format <b>Content-Type:</b> application/my-format.</p> <p>To hide values in the POST data, add a line to the <b>master.config</b> file, such as:</p> <pre>_private=_name=mysecret _value=rosebud _private=_name=mypassword _privateValue=sesame</pre> <p>and then use the following form in the POST data:</p> <pre>s username=\$private-mysecret\$  s password=\$private-mypassword\$ </pre> <p>and SiteScope substitutes the values from the <b>master.config</b> into the POST data.</p>
<b>POST data encoding</b>	<p>Determines if the POST data is encoded. Select from the following options:</p> <ul style="list-style-type: none"> <li>➤ <b>Use content type.</b> Decide to encode the POST data by the content type header. If the header equals urlencoded then encode, otherwise do not encode.</li> <li>➤ <b>Force URL encoding.</b> Always encode the post data.</li> <li>➤ <b>Do not force URL encoding.</b> Do not encode the POST data.</li> </ul>



GUI Element	Description
<p><b>Check for content changes</b></p>	<p>SiteScope records a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs.</p> <p>If the checksum changes, the monitor has a status of <b>content changed error</b> and goes into error. If you want to check for content changes, you usually want to use <b>Compare to saved contents</b>.</p> <p>The options for this setting are:</p> <ul style="list-style-type: none"> <li>▶ <b>No content checking</b> (default). SiteScope does not check for content changes.</li> <li>▶ <b>Compare to last contents</b>. The new checksum is recorded as the default after the initial error <b>content changed error</b> occurs, so the monitor returns to OK until the checksum changes again.</li> <li>▶ <b>Compare to saved contents</b>. The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor gets a <b>content changed error</b> and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents.</li> <li>▶ <b>Reset saved contents</b>. Takes a new snapshot of the page and saves the resulting checksum on the first monitor run after this option is chosen. After taking the snapshot, the monitor reverts to <b>Compare to saved contents</b> mode.</li> </ul> <p><b>Default value:</b> No content checking</p>
<p><b>HTTP version</b></p>	<p>Select the HTTP version for SiteScope to use for style request headers (HTTP version 1.1 or 1.0).</p> <p><b>Default value:</b> 1.1</p>

GUI Element	Description
<b>Retrieve images</b>	<p>Select if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by IMG, BODY (from the background property), and INPUT TYPE=IMAGE HTML tags.</p> <p>Images that appear more than once in a page are retrieved only once.</p> <p><b>Note:</b> If this option is checked, each image referenced by the target URL contributes to the download time. However, if a image times out during the download process or has a problem during the download, that time is not added to the total download time.</p> <p><b>Default value:</b> Not selected</p>
<b>Retrieve frames</b>	<p>Select if you want SiteScope to retrieve the frames references in a frameset and count their retrieval time in the total time to download this page. Frames include those referenced by FRAME and IFRAME tags.</p> <p>If <b>Retrieve images</b> is also checked, SiteScope attempts to retrieve all images in all frames.</p> <p><b>Note:</b> If this option is checked, each frame referenced by the target URL contributes to the download time. However, if a frame times out during the download process or has a problem during the download, that time is not added to the total download time.</p> <p><b>Default value:</b> Not selected</p>
<b>Error if redirected</b>	<p>Select to have SiteScope generate an error (and notify you) if a URL is redirected.</p> <p><b>Default value:</b> Not selected</p>

GUI Element	Description
<b>Use WinInet</b>	<p>Select to use WinInet as an alternative HTTP client for this monitor.</p> <p>Select this option to use WinInet instead of Apache when:</p> <ul style="list-style-type: none"> <li>▶ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates while Apache does not.</li> <li>▶ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.</li> </ul> <p><b>Default value:</b> Not selected</p>
<b>Authentication Settings</b>	
<b>Credentials</b>	<p>If the URL specified requires a name and password for access, select the option to use for authorizing credentials:</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the URL in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password for the URL (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>

GUI Element	Description
<b>Pre-emptive authorization</b>	<p>Select when the authorization credentials should be sent if SiteScope requests the target URL.</p> <ul style="list-style-type: none"> <li>➤ <b>Use global preference.</b> Select to have SiteScope use the setting specified in the <b>Pre-emptive authorization</b> section of the General Preferences page.</li> <li>➤ <b>Authenticate first request.</b> Select to send the user name and password on the first request SiteScope makes for the target URL. <ul style="list-style-type: none"> <li><b>Note:</b> If the URL does not require a user name and password, this option may cause the URL to fail.</li> </ul> </li> <li>➤ <b>Authenticate if requested.</b> Select to send the user name and password on the second request if the server requests a user name and password. <ul style="list-style-type: none"> <li><b>Note:</b> If the URL does not require a user name and password, this option may be used.</li> </ul> </li> </ul> <p>All options use the <b>User name</b> and <b>Password</b> entered for this monitor instance. If these are not specified for the individual monitor, the <b>Default authentication user name</b> and <b>Default authentication password</b> specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p><b>Note:</b> Pre-emptive authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
<b>Accept untrusted certificates for HTTPS</b>	<p>If you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope does not have the required server certificates, you can either select this option or import the related certificates. For details on importing server certificates, see SSL Connectivity in “URL Monitor Overview” on page 941.</p>
<b>Accept invalid certificates for HTTPS</b>	<p>Select this option if you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope has invalid server certificates. This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.</p>

GUI Element	Description
<b>Client side certificate</b>	<p>If you need to use a client side certificate to access the target URL, select the certificate file using the drop down menu. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You enter the password for the certificate in the <b>Client side certificate password</b> box.</p> <p><b>Note:</b> Client side certificate files must be copied into the &lt;SiteScope root directory&gt;\templates.certificates directory.</p>
<b>Client side certificate password</b>	<p>If you are using a client side certificate and that certificate requires a password, enter the password.</p>
<b>Authorization NTLM domain</b>	<p>Enter the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL.</p>
<b>NTLM V2</b>	<p>Select if the URL you are accessing requires authentication using NTLM version 2.</p>
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	<p>A proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.</p>
<b>Proxy server user name</b>	<p>If the proxy server requires a user name to access the URL, enter the name here.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy server password</b>	<p>If the proxy server requires a password to access the URL, enter the password here.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy NTLM V2</b>	<p>Select if the proxy requires authentication using NTLM version 2.</p>



# 91

---

## URL Content Monitor

This chapter includes the main concepts, tasks, and reference information for the URL Content monitor.

### **This chapter includes:**

#### Concepts

- ▶ URL Content Monitor Overview on page 959

#### Tasks

- ▶ Configure the URL Content Monitoring Environment on page 962

#### Reference

- ▶ URL Content Monitor Settings on page 963

### **URL Content Monitor Overview**

The URL Content monitor is primarily used to monitor Web pages that are generated dynamically and display statistics about custom applications. By monitoring these pages, these statistics can be retrieved and integrated into the rest of your SiteScope system. The URL Content monitor supports monitoring HTTP versions 1.0 and 1.1.

You should use the URL Content monitor if you need to verify multiple values (up to 10 variables) from the content of a single URL. Otherwise, the standard URL monitor is normally used. One use for this monitor is to integrate SiteScope with other applications that export numeric data through a Web page. The content values are matched using regular expressions. The monitor includes the matched values as part of the monitor status which are written to the log. If the matched values are numeric data, the results can be plotted in a report.

This section contains the following topics:

- “Status” on page 960
- “Scheduling the Monitor” on page 961
- “Setup Requirements and User Permissions” on page 961
- “SSL Connectivity” on page 961
- “Troubleshooting and Limitations” on page 962
- “Configuring the Monitor” on page 962

### **Status**

Each time the URL Content monitor runs, it returns a status and several match values and writes them in the monitoring log file. It also writes the total time it takes to receive the designated document in the log file.

The reading is the current value of the monitor. Possible values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error
- document moved
- unauthorized



- forbidden
- not found
- proxy authentication required
- server error
- not implemented
- server busy

The status is displayed as good, warning, or error in the Dashboard dependent on the results of the retrieval, content match, and the error or warning status criteria that you select.

## Scheduling the Monitor

The frequency depends on the statistics being monitored. For most statistics, every several minutes is often sufficient.

## Setup Requirements and User Permissions

The user name and password specified in the **Credentials** section must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.

## SSL Connectivity

Web servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The `http://` prefix means that the server uses a non-encrypted connection. The `https://` prefix means that it is a secure, encrypted connection. Monitoring a Web server which uses an encrypted connection, requires either:

- Selecting the **Accept untrusted certificates for HTTPS** option in the Authentication Settings section of the Monitor Settings panel as described in “URL Content Monitor Settings” on page 963.
- Importing the server certificate. For details on how to perform this task, see “Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)” on page 962.

## Troubleshooting and Limitations

You can use the URL Sequence Tool to get on the spot data for the URL and to view the HTML received from the HTTP request.

## Configuring the Monitor

For task details, see “Configure the URL Content Monitoring Environment” on page 962.

For user interface details, see “URL Content Monitor Settings” on page 963.

## Configure the URL Content Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- ▶ “Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)” on page 962
- ▶ “Configure the Monitor Properties” on page 963

### **1 Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)**

If the Web server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate. Use one of the following methods for importing server certificates:

- ▶ Import the server certificates using SiteScope Certificate Management. For details, see “Import Server Certificates Using Certificate Management” on page 1537.
- ▶ Import the server certificates manually. For details, see “Import Server Certificates Manually” on page 947.

## 2 Configure the Monitor Properties

Complete the URL Content monitor configuration. For details on the monitor settings, see “URL Content Monitor Settings” on page 963.

### URL Content Monitor Settings

<b>Description</b>	<p>The URL Content monitor is a specialized variation of the URL Monitor that can match up to ten different values from the content of a specified URL. The matched values are displayed with the status of the monitor in the monitor group table and written to the monitor log.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>URL Tool</b> is available when configuring this monitor to request a URL from a server, print the returned data, and test network routing (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “URL Tool” on page 247.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the URL Content Monitoring Environment” on page 962</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “URL Content Monitor Overview” on page 959</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## URL Content Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Setting</b>	
<b>URL</b>	<p>Enter the URL that you want to monitor.</p> <p><b>Example:</b> http://demo.thiscompany.com</p> <p>If you are monitoring a secure URL, the URL must reflect the correct transfer protocol. The URL starts with https:// and the connection is made using SSL.</p> <p><b>Example:</b> https://demo.thiscompany.com</p>
<b>Match content</b>	<p>Enter an expression describing the values to match in the returned page. If the expression is not contained in the page, the monitor displays the message no match on content. A regular expression is used to define the values to match.</p> <p>Use parentheses to allow the monitor to retrieve these values as counters. By using the labels, these counters can be automatically assigned with a customized name and you can define thresholds for them. You can use up to 10 sets of parentheses.</p> <p><b>Example:</b> The expression /Copyright (\d*)-(\d*)/ would match two values, 1996 and 1998, from a page that contained the string Copyright 1996-1998. The returned values (1996 and 1998) could be used when setting Error if or Warning if thresholds.</p> <p><b>Note:</b> You can click the <b>Open Tool</b> button to use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</p>

GUI Element	Description
<b>Match content labels</b>	<p>Use this option to enter labels for the matched values found in the content. The matched value labels are used as variables to access retained values from the content match expression for use with the monitor threshold settings. These labels are also displayed as the text labels in graphs generated for the retained values in management reports for this monitor.</p> <p><b>Example:</b> Type Copyright_start, Copyright_end to represent the copyright date range used in the <b>Match content</b> field. After the monitor runs, these labels are displayed in the Condition list in Threshold Settings, enabling you to set status threshold settings (Error if, Warning if, and Good if) for the matched value.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ Separate multiple labels with a comma (,).</li> <li>▶ You can set up to 10 labels.</li> </ul>
<b>Match content for error</b>	<p>Enter a string of text to check for in the returned page. If the text is contained in the page, the monitor displays content error found. HTML tags are part of a text document, so include them if they are part of the text for which you are searching.</p> <p><b>Example:</b> &lt; B&gt; Error &lt; /B&gt; Message</p> <p>You can also perform a regular expression match by enclosing the string in forward slashes, with an <b>i</b> after the trailing slash, to indicate that there is no case sensitive matching. Click the <b>Open Tool</b> button to use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression Tool” on page 232.</p> <p><b>Example:</b> /href=Doc\d+\.html/ or /href=doc\d+\.html/i</p> <p><b>Note:</b> The search is case sensitive.</p>

GUI Element	Description
<b>Show detailed measurement</b>	<p>Select if you want SiteScope to record a detailed breakdown of the process times involved in retrieving the requested URL. These times include the following:</p> <ul style="list-style-type: none"> <li>▶ <b>DNS lookup time.</b> The time it takes to send a name resolution request to your DNS server until you get a reply.</li> <li>▶ <b>Connection time.</b> The time it takes to establish a TCP/IP/Socket connection to the Web server.</li> <li>▶ <b>Server response time.</b> The time after the request is sent until the first byte (rather first buffer full) of the page comes back.</li> <li>▶ <b>Download time.</b> The time it takes to download the entire page.</li> </ul>
<b>Timeout (seconds)</b>	<p>The number of seconds that the URL monitor should wait for a page to begin downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status.</p> <p>If you have selected the <b>Retrieve frames</b> or <b>Retrieve images</b> option, SiteScope waits for these items to be retrieved before considering the page to be fully downloaded.</p> <p><b>Default value:</b> 60 seconds</p>
<b>Retries</b>	<p>Enter the number of times that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request for is a recoverable error.</p> <p><b>Default value:</b> 0</p>

GUI Element	Description
<b>HTTP Settings</b>	
<b>Request headers</b>	<p>The header request lines sent by the HTTP client to the server. Headers should be separated by a linebreak. The standard list of HTTP1.1 request headers can be found in <a href="http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14">http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14</a>.</p> <p><b>Note:</b> Although this field is optional, some Web pages behave unexpectedly when the request header is missing (such as performing endless redirects, providing wrong content, and so forth).</p>
<b>URL content encoding</b>	<p>SiteScope retrieves the correct encoding from the server response. The default value appearing here should not be edited.</p> <p><b>Default value:</b> Retrieve encoding from server response</p>
<b>POST data</b>	<p>If the URL is for a POST request, enter the post variables, one per line as name=value pairs. This option is used to verify that a form is working correctly by performing the same request that occurs when a user submits a form.</p> <p>See also the Match Content box for a way to verify that the correct form response was received.</p> <p>If this item is blank, a GET request is performed.</p> <p><b>Note:</b> This item can also be used to pass cookies with the request.</p> <p><b>Example:</b> "Set-cookie:&lt;cookieName&gt;=&lt;cookieValue&gt;"</p>
<b>POST data encoding</b>	<p>Determines if the POST data is to be encoded. Select from the following options:</p> <ul style="list-style-type: none"> <li>▶ <b>Use content type.</b> Decide to encode the post data by the content type header. If the header equals <b>urlencoded</b> then encode, otherwise do not encode.</li> <li>▶ <b>Force URL encoding.</b> Always encode the POST data.</li> <li>▶ <b>Do not force URL encoding.</b> Do not encode the POST data.</li> </ul> <p><b>Default value:</b> Use content type</p>

GUI Element	Description
<b>Check for content changes</b>	<p>SiteScope records a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs.</p> <p>If the checksum changes, the monitor has a status of <b>content changed error</b> and go into error. If you want to check for content changes, you usually want to use <b>compare to saved contents</b>.</p> <p>The options for this setting are:</p> <ul style="list-style-type: none"> <li>➤ <b>No content checking</b> (default). SiteScope does not check for content changes.</li> <li>➤ <b>Compare to last contents</b>. The new checksum is recorded as the default after the initial error <b>content changed error</b> occurs, so the monitor returns to OK until the checksum changes again.</li> <li>➤ <b>Compare to saved contents</b>. The checksum is a snapshot of a given page (retrieved either during the initial or a specific run of the monitor). If the contents change, the monitor gets a <b>content changed error</b> and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents.</li> <li>➤ <b>Reset saved contents</b>. Takes a new snapshot of the page and saves the resulting checksum on the first monitor run after this option is chosen. After taking the snapshot, the monitor reverts to <b>Compare to saved contents</b> mode.</li> </ul> <p><b>Default value:</b> No content checking</p>
<b>HTTP version</b>	<p>Select the HTTP version for SiteScope to use for style request headers (HTTP version 1.0 or 1.1).</p> <p><b>Default value:</b> 1.1</p>



GUI Element	Description
<b>Retrieve images</b>	<p>Select if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by IMG, BODY (from the background property), and INPUT TYPE=IMAGE HTML tags. Images that appear more than once in a page are only retrieved once.</p> <p><b>Note:</b> If the Retrieve Images option is checked, each image referenced by the target URL contributes to the download time. However, if an image times out during the download process or has a problem during the download, that time is not added to the total download time.</p>
<b>Retrieve frames</b>	<p>Select if you want SiteScope to retrieve the frames references in a frameset and count their retrieval time in the total time to download this page. Frames include those referenced by FRAME and IFRAME tags.</p> <p>If <b>Retrieve images</b> is also checked, SiteScope attempts to retrieve all images in all frames.</p> <p><b>Note:</b> If the <b>Retrieve frames</b> option is checked, each frame referenced by the target URL contributes to the download time. However, if a frame times out during the download process or has a problem during the download, that time is not added to the total download time.</p>
<b>Error if redirected</b>	<p>Select if you want SiteScope to notify you if a URL is redirected.</p>

GUI Element	Description
<p><b>Use WinInet</b></p>	<p>Select to use WinInet as an alternative HTTP client for this monitor.</p> <p>Select this option to use WinInet instead of Apache when:</p> <ul style="list-style-type: none"> <li>▶ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates while Apache does not.</li> <li>▶ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.</li> </ul> <p><b>Note:</b> This field is available on Windows versions of SiteScope only.</p>
<p><b>Authentication Settings</b></p>	
<p><b>Credentials</b></p>	<p>If the URL specified requires a name and password for access, select the option to use for authorizing credentials:</p> <ul style="list-style-type: none"> <li>▶ <b>Use use name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the URL in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password for the URL. Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>

GUI Element	Description
<b>Pre-emptive authorization</b>	<p>Select when the authorization credentials should be sent if SiteScope requests the target URL.</p> <ul style="list-style-type: none"> <li>▶ <b>Use global preference.</b> Select to have SiteScope use the <b>When to Authenticate</b> setting as specified in the Pre-emptive Authorization section of the General Preferences page.</li> <li>▶ <b>Authenticate first request.</b> Select to send the user name and password on the first request SiteScope makes for the target URL. <ul style="list-style-type: none"> <li><b>Note:</b> If the URL does not require a user name and password, this option may cause the URL to fail.</li> </ul> </li> <li>▶ <b>Authenticate if requested.</b> Select to send the user name and password on the second request if the server requests a user name and password. <ul style="list-style-type: none"> <li><b>Note:</b> If the URL does not require a user name and password, this option may be used.</li> </ul> </li> </ul> <p>All options use the <b>User name</b> and <b>Password</b> entered for this monitor instance. If these are not specified for the individual monitor, the <b>Default authentication user name</b> and <b>Default authentication password</b> specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p><b>Note:</b> Pre-emptive authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
<b>Accept untrusted certificates for HTTPS</b>	<p>If you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope does not have the required server certificates, you can either select this option or import the related certificates. For details on importing server certificates, see SSL Connectivity in “URL Content Monitor Overview” on page 959.</p>
<b>Accept invalid certificates for HTTPS</b>	<p>Select this option if you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope has invalid server certificates. This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.</p>

GUI Element	Description
<b>Client side certificates</b>	<p>If you need to use a client side certificate to access the target URL, select the certificate file using the drop down menu. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You type the password for the certificate in the <b>Client side cert password</b> box.</p> <p><b>Note:</b> Client side certificate files must be copied into the &lt;SiteScope root directory&gt;\templates.certificates directory.</p>
<b>Client side certificates password</b>	<p>If you are using a client side certificate and that certificate requires a password, enter the password.</p>
<b>Authorization NTLM domain</b>	<p>Enter the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL.</p>
<b>NTLM V2</b>	<p>Select if the URL you are accessing requires authentication using NTLM version 2.</p>
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	<p>A proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.</p>
<b>Proxy server user name</b>	<p>If the proxy server requires a user name to access the URL, enter the name here.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy server password</b>	<p>If the proxy server requires a password to access the URL, enter the password here.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy NTLM V2</b>	<p>Select if the proxy requires authentication using NTLM version 2.</p>

# 92

---

## URL List Monitor

This chapter includes the main concepts, tasks, and reference information for the URL List monitor.

### **This chapter includes:**

#### Concepts

- ▶ URL List Monitor Overview on page 973

#### Tasks

- ▶ Configure the URL List Monitoring Environment on page 977

#### Reference

- ▶ URL List Monitor Settings on page 978

### **URL List Monitor Overview**

You can use the URL List monitor to check the availability of a list of URLs without having to create a separate URL monitor for each one. For example, this is useful if you host several Web sites and simply want to see that they are each serving pages as expected. The URL List monitor is not used to confirm links between pages (see the “Link Check Monitor Overview” on page 591) or other Web transaction processes (see “URL Sequence Monitor Overview” on page 983). The URL List monitor supports monitoring HTTP versions 1.0 and 1.1.

A URL List is specified by giving a filename containing the list of URLs to check. The URLs that you want to monitor are saved in a plain text file. There is virtually no limit to the number that you can list though the run interval selected for the monitor may require that the number of URLs be limited. For each URL included in the URL list file, the monitor retrieves the contents of the URL or the server response to the request.

This section contains the following topics:

- “Scheduling the Monitor” on page 974
- “Setup Requirements and User Permissions” on page 975
- “SSL Connectivity” on page 976
- “Troubleshooting and Limitations” on page 976
- “Configuring the Monitor” on page 976

### **Scheduling the Monitor**

This is strictly dependent on how often you want to check to see if the URLs are working. Once an hour is common, but you can schedule it to run more often.

There are a few factors that affect how long it takes the URL List monitor to complete a run:

- number of URLs in the list
- URL retrieval time
- the number of threads used

In some cases this may lead to the monitor not running as expected. As an example, assume you have a list of 200 URLs that you want to monitor every 10 minutes, but, due to Internet traffic, SiteScope is not able to complete checking all of the 200 URLs in that amount of time. The next time the monitor was scheduled to run, SiteScope would see that it did not complete the previous run and would wait for another 10 minutes before trying again.

The error log marks this as a "skip". If this happens 10 times, SiteScope restarts itself, and SiteScope Health shows an error status. There are several things you can do to try to resolve this issue:

- ▶ Schedule the monitor to run less frequently. If this conflicts with some other objective, use the other options.
- ▶ Split the URLs that you want to check into more than one list, and add additional monitors to monitor each list.
- ▶ Increase the number of threads that SiteScope can use when checking the URLs. The more threads, the quicker SiteScope can check them. Increasing the number of threads can adversely affect SiteScope's performance.

Ideally, you want SiteScope to have just completed checking the URLs in the list when it is time to start checking again. This would indicate that the load was evenly balanced.

Each time the URL List monitor runs, it returns the number of errors, if any, and writes it into the monitoring log file. It also writes the total number of URLs checked and the average time, in milliseconds, to retrieve each URL.

### **Setup Requirements and User Permissions**

The user name and password specified in the **Credentials** section must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.

## SSL Connectivity

Web servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The `http://` prefix means that the server uses a non-encrypted connection. The `https://` prefix means that it is a secure, encrypted connection. Monitoring a Web server which uses an encrypted connection, requires either:

- ▶ Selecting the **Accept untrusted certificates for HTTPS** option in the Authentication Settings section of the Monitor Settings panel as described in “URL List Monitor Settings” on page 978.
- ▶ Importing the server certificate. For details on how to perform this task, see “Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)” on page 977.

## Troubleshooting and Limitations

You can use the URL Sequence Tool to get on the spot data for the URL and to view the HTML received from the HTTP request.

## Configuring the Monitor

For task details, see “Configure the URL List Monitoring Environment” on page 977.

For user interface details, see “URL List Monitor Settings” on page 978.



## **Configure the URL List Monitoring Environment**

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)” on page 977
- “Configure the Monitor Properties” on page 977

### **1 Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)**

If the Web server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate. Use one of the following methods for importing server certificates:

- Import the server certificates using SiteScope Certificate Management. For details, see “Import Server Certificates Using Certificate Management” on page 1537.
- Import the server certificates manually. For details, see “Import Server Certificates Manually” on page 947.

### **2 Configure the Monitor Properties**

Complete the URL List monitor configuration. For details on the monitor settings, see “URL List Monitor Settings” on page 978.

## URL List Monitor Settings

<b>Description</b>	<p>The URL List monitor is used to check a large list of URLs. This monitor is commonly used by Web hosting providers to measure the availability and performance of their customer's Web sites.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the URL List Monitoring Environment” on page 977</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “URL List Monitor Overview” on page 973</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### URL List Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>URL list file</b>	<p>Enter the path for the file containing the list of URLs to be monitored. This file should be a plain text file and contain only one URL per line.</p> <p><b>Examples:</b></p> <p><code>http://www.website.com/index.html</code>  <code>http://www.website.com/main/customer/order.html</code>  <code>http://www.website.net/default.htm</code>  <code>http://www.Webpages.com/tech/support/ws/intro.html</code></p>

GUI Element	Description
<b>Log file</b>	Enter the path for the log file for this monitor. For each URL checked, an entry is added to this log file. If this item is blank, a log is not created.
<b>Error log file</b>	Enter the path for the error log file for this monitor. For each error retrieving a URL, an entry is added to this log file. If this item is blank, a log is not created.
<b>Specific server</b>	Optionally, if the URL file is not a text file, you can enter the Server name to specify which URLs to check in the URL list. If the URLs are stored in a map format, this item is used to check a subset of the URLs from the list. <b>Default value:</b> All URLs that are in the list are checked. <b>Note:</b> If you modify the value in the this box, you must also change the value in the <b>URL list file</b> box for SiteScope to implement the change.
<b>Pause (milliseconds)</b>	Enter the pause, in milliseconds, between each URL check. Decreasing this number shortens the total time required to check all of the URLs but also increases the load on the server. <b>Default value:</b> 1000 milliseconds
<b>Threads</b>	Enter the number of threads to retrieve URLs. This is the number of simultaneous checks to perform. Increasing this number shortens the time for all of the URLs to be checked but also increases the load on the server. <b>Default value:</b> 4
<b>Timeout (seconds)</b>	The number of seconds that the URL monitor should wait for a page to complete downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status. <b>Default value:</b> 60 seconds
<b>Retries</b>	Enter the number of times you want SiteScope to try to reach URLs that are returning an error. <b>Default value:</b> 0

GUI Element	Description
<b>HTTP Settings</b>	
<b>Request headers</b>	<p>The header request lines sent by the HTTP client to the server. Headers should be separated by a linebreak. The standard list of HTTP1.1 request headers can be found in <a href="http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14">http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14</a>.</p> <p><b>Note:</b> Although this field is optional, some Web pages behave unexpectedly when the request header is missing (such as performing endless redirects, providing wrong content, and so forth).</p>
<b>Use WinInet</b>	<p>Select to use WinInet as an alternative HTTP client for this monitor.</p> <p>Select this option to use WinInet instead of Apache when:</p> <ul style="list-style-type: none"> <li>▶ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates while Apache does not.</li> <li>▶ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.</li> </ul> <p><b>Default value:</b> Not selected</p>
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	(Optional) A proxy server can be used to access the URLs in the list. Enter the domain name and port of an HTTP Proxy Server.
<b>Proxy server user name</b>	<p>If the proxy server requires a user name to access the URL, enter the name here.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>

GUI Element	Description
<b>Proxy server password</b>	<p>If the proxy server requires a password to access the URL, enter the password here.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Authentication Settings</b>	
<b>Credentials</b>	<p>If the URLs in the list require a user name and password for access, select the option to use for authorizing credentials:</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password to access the URLs in the <b>User name</b> and <b>Password</b> box.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password for the URLs (default option). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>



# 93

---

## URL Sequence Monitor

This chapter includes the main concepts, tasks, and reference information for the URL Sequence monitor.

### **This chapter includes:**

#### Concepts

- ▶ URL Sequence Monitor Overview on page 983

#### Tasks

- ▶ Create a URL Sequence on page 997

#### Reference

- ▶ URL Sequence Monitor User Interface on page 1000

### **URL Sequence Monitor Overview**

You use URL Sequence Monitors to verify that multiple-page Web transactions are working properly. This is an important part of monitoring key business processes and services. For example, you can have SiteScope retrieve a login page, type an account name by using a secure Web form, check an account status for the page that is returned, and then follow a sequence of links through several more pages. URL Sequence Monitors are also useful for checking pages that include dynamically generated information, such as session IDs, that are embedded in the Web pages by using dynamic links or hidden input items. The URL Sequence monitor supports monitoring HTTP versions 1.0 and 1.1.

The core of the URL Sequence monitor is the sequence of URL and associated action requests that are performed by the monitor. A URL Sequence begins with a URL acting as the starting point or Step 1 for the sequence. This can then be followed by additional URLs that are accessed manually, or more commonly, by links or form buttons that a user would select to navigate or complete a specific transaction.

By default, you can define up to twenty sequence steps. For each step you may specify a content match to search for, enter a user name and password if required, define custom POST data, as well as other optional criteria for that step.

You can edit the steps in a URL sequence after they have been added. Making changes to a sequence step requires that you update both the individual step and update the monitor as a whole. Editing any step of a URL sequence may affect subsequent steps in the sequence and cause the sequence to fail. It may be necessary to change all of the steps that occur after the step that is changed.

You can delete steps from a URL sequence but they can only be deleted starting from the last step in the sequence. This is to prevent inadvertently breaking a sequence because, in most cases, one step is dependent on data returned by the previous step. When you update or delete steps, SiteScope attempts to run the changes to the step. The results of the monitor run are displayed in SiteScope Dashboard.

This section contains the following topics:

- ▶ “What to Monitor” on page 985
- ▶ “Working with the URL Sequence Monitor” on page 985
- ▶ “Setup Requirements and User Permissions” on page 987
- ▶ “Defining Sequence Steps” on page 987
- ▶ “SSL Connectivity” on page 989
- ▶ “URL Sequences and Dynamic Content” on page 990
- ▶ “Retaining and Passing Values Between Sequence Steps” on page 994
- ▶ “Sharing Cookies Between Monitor Runs and Configured Monitors” on page 995



- “Troubleshooting and Limitations” on page 996
- “Configuring the Monitor” on page 996

## What to Monitor

You should monitor any multi-step Web page sequence that you have made available to general users to verify that they are available and function correctly. Web site visitors often assume that any problems they encounter are due to user error rather than system error, especially if they're not familiar with your application. By using this monitor to perform sequence testing, you can verify that users are able to successfully complete transactions.

## Working with the URL Sequence Monitor

The URL Sequence monitor is more complex than most other SiteScope monitor types and the steps for working with the monitor are different than for other monitors. The following is an overview of key concepts and actions you use when working with the URL Sequence monitor:

- The URL Sequence monitor can be configured with between one to forty steps. Each step is defined individually in a sequence of numbered entries in the interface. The steps must be initially configured in the intended sequence as the request for one step provides the content used in the following step.
- When you first configure a URL Sequence monitor, be sure to configure the steps you want to include in the sequence before you create the monitor.
- You can set thresholds for individual steps or for the whole monitor.
- You configure the URL Sequence monitor in text mode. The navigation links and form actions are displayed as text parsed from the HTML that is used to construct a page in Web browsers. In some cases, portions of HTML code may also be included. You must be familiar with HTML when working with this monitor.

- ▶ Many Web-based systems use session data to identify clients and track the state of a user's interaction with the server application. This session data is often sent back and forth to the client in the HTTP header or Post Data. You should be familiar with the session tracking methods used by the systems you want to monitor to effectively configure this monitor.
- ▶ Web-based sequences or transactions can be difficult to navigate when dealing with many Web pages. For example, Web pages that use many graphic images for navigation hyperlinks can present special challenges when configuring URL Sequence monitors. You must be familiar with HTML hyperlink syntax when working with this monitor.
- ▶ When you first configure the URL Sequence monitor, the HTML text content returned from the request made in one step can be displayed in the following step by clicking the **Show Source** button. This can be very useful for finding content on which you want to perform a match. You may also use this to correlate links and forms in the respective selection menus with their relative location on the page. For example, if there is a search entry form near the top of a Web page and another, different search form further down in the page, you can view the raw HTML to help determine the syntax associated with the form that you want to test.
- ▶ SiteScope does not parse or interpret embedded scripts or other client-side program code such as Javascript (ECMAScript). Web page content that is generated or controlled by client-side code does not usually appear in the URL Sequence monitor. For information about dealing with Web page scripts, see "URL Sequence Monitor Settings" on page 1000 and Client-side Programs help page.
- ▶ You should consider using the VuGen script rather than the URL Sequence monitor in the following circumstances:
  - ▶ Where Javascripts are embedded in the HTML being monitored (if they play an important role in the HTML). This is because Javascripts are not supported by the URL monitor.
  - ▶ If you experience problems when monitoring HTMLs over the SSL protocol, and these problems persist after you have verified that all monitor settings are correct.

## Setup Requirements and User Permissions

The user name and password specified in the URL Sequence Step dialog box must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.

## Defining Sequence Steps

The URL sequence must begin with an initial URL. SiteScope makes a request for the URL, and the data returned by this initial request is used for subsequent steps. The HTTP response header and the content of the URL are available in the HTML Source section at the bottom of the subsequent step dialog box.

When you have entered the first step, you can add more steps. You repeat this process depending on the number of Web pages and actions that need to be taken to complete the sequence. The step screens provide access to the available elements on the Web page requested by the previous step. This includes form buttons, hyperlinks, form input elements, and other data. You use these elements to create each subsequent sequence step separately. Most sequence steps involve one of the following elements:

Reference Type	Description
Go to URL Manually	Where the sequence uses the Common Gateway Interface (CGI) for data transmission between the client and the server, it may be useful to specify a particular URL and name-value pairs. You can enter the URL you want to request along with any name-value pairs needed to get to the next sequence step even if those values are available through some other page element (such as a form). This option also enables you to copy URL and CGI strings directly from the location or address bar of another browser client that you may be using to step through the sequence you are building.

Reference Type	Description
Following a Hyperlink	<p>SiteScope parses the content of the URL returned by the previous step and creates a list of hyperlinks that are found on the page. This includes links that are part of an image map that may be virtual "buttons" on a navigation menu. Any links found on this page of the sequence can be viewed and selected using the drop-down list box to the right of the <b>Link</b> radio button. Use the following steps to add a link step to the sequence.</p>
Selecting a Form button	<p>SiteScope parses the content of the URL in the current step and creates a list of form elements of the type "Submit". If SiteScope finds any HTML forms on the current page of the sequence, they are displayed in a drop-down list.</p> <p>The listings are in the following format: {[formNumber]FormName)ButtonName</p> <p><b>Example:</b> The Search button on a company's search page might be listed  as: {[1]http://www.CompanyName.com/bin/search}search</p>
Selecting a Frame within a frameset	<p>If the URL for a step in the sequence contains an HTML FRAMESET and you need to access a hyperlink, form, or form button that is a page displayed in a frame, you must drill down into the Frameset to the actual page that contains the links or forms that you want before you can proceed with other steps in the sequence.</p>
Following a META REFRESH redirection	<p>If the page for this step of the sequence is controlled by a &lt;META HTTP-EQUIV="Refresh" CONTENT="timedelay; URL=filename.htm"&gt; tag, you can instruct SiteScope to retrieve the specified file as the next step. This sort of construct is sometimes used for intro pages, splash screens, or pages redirecting visitors from an obsolete URL to the active URL.</p>

---

**Note:** SiteScope does not parse or interpret embedded scripts or other client-side program code such as Javascript (ECMAScript). Web page content that is generated or controlled by client-side code usually does not appear in the URL Sequence monitor.

---

## SSL Connectivity

Web servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The `http://` prefix means that the server uses a non-encrypted connection. The `https://` prefix means that it is a secure, encrypted connection. Monitoring a Web server which uses an encrypted connection, requires either:

- ▶ Selecting the **Accept untrusted certificates for HTTPS** option in the Authentication Settings section of the URL Sequence Monitor Settings panel as described in “URL Sequence Monitor Settings” on page 1000.
- ▶ Importing the server certificate. For details on how to perform this task, see “Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)” on page 997.

## **URL Sequences and Dynamic Content**

Web pages which include client-side programming or dynamically generated content can present problems in constructing SiteScope URL Sequence monitors. Client-side programs might include Java applets, ActiveX controls, Javascript, or VBScript. Web pages which are generated by server-side programming (Perl/CGI, ASP, CFM, SSI, JSP, and so forth) can also present a problem if link references or form attributes are changed frequently.

SiteScope does not interpret Javascript, VBScript, Java applets, or Active X Controls embedded in HTML files. This may not be a problem when the functionality of the client-side program is isolated to visual effects on the page where it is embedded. Problems can arise when the client-side program code controls links to other URL's or modifies data submitted to a server-side program. Because SiteScope does not interpret client-side programs, actions or event handlers made available by scripts or applets are not displayed in the URL Sequence Step dialog box.

Some Web sites use dynamically generated link references on pages generated by server-side programming. While these Web pages do not contain client-side programs, frequently changing link references or cookie data can make it difficult to set up and maintain a URL Sequence monitor.

## Dynamic Content Workarounds

There are several ways to make a SiteScope URL Sequence monitor perform actions controlled by client-side programs and other dynamic content. Several of these workarounds are presented below. The workarounds generally require knowledge of the principles of Web page construction, CGI programming, Perl-style regular expressions, and the programming used to support the Web site being monitored.

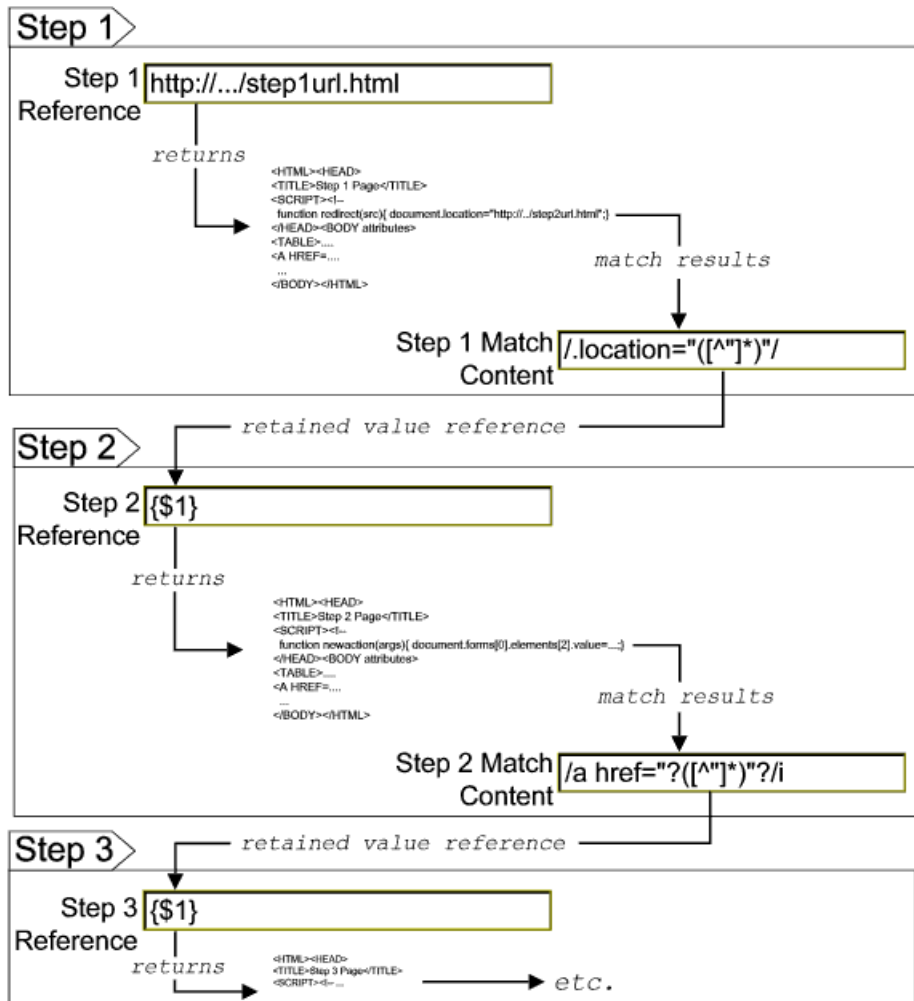
Dynamic Content	SiteScope Workaround
<p>A Web page contains a script which controls a link to another URL.</p> <p><b>Example:</b> onClick = "document.location='http://..."</p>	<p>Use a match content regular expression in the sequence step for the subject page to retain the <b>filename.ext</b> value from the <code>.location="filename.ext"</code> match pattern. The retained value can then be passed as a URL in the <b>URL</b> box of the next step of the sequence.</p>
<p>A client-side program reformats, edits, or adds data to a POST or GET data set collected by HTML form inputs.</p>	<p>Manually edit the script changes into the <b>NAME=VALUE</b> pairs displayed for the subject sequence step. This is done in the <b>POST data</b> box in the HTTP Settings section of the URL Sequence Step dialog box. This requires familiarity with the script function and CGI request headers.</p>
<p>A client-side program generates HTML content which, after interpretation by a Web browser, includes HTML <code>&lt;A HREF=...&gt;</code> links.</p>	<p>Use a match content regular expression to return the <code>filename.ext</code> value from the <code>HREF="filename.ext"</code> pattern and pass it to the <b>URL</b> box of the next sequence step.</p>

Dynamic Content	SiteScope Workaround
A client-side program generates HTML content which, after interpretation by a Web browser, includes forms submitted to a CGI program.	Manually enter the NAME=VALUE pairs for the subject sequence step. This is done in the <b>POST data</b> box in the HTTP Settings section of the URL Sequence Step dialog box. This requires familiarity with the script, the form structure, and CGI request headers.
A script dynamically sets the ACTION attribute of an HTML <FORM> tag.	Manually enter the ACTION URL for the next sequence step. This is done in the <b>URL</b> box in the Reference Settings section of the URL Sequence Step dialog box. This requires familiarity with the script.
A script dynamically sets the METHOD attribute of an HTML <FORM> tag.	Manually enter the POST or GET data for the next sequence step. For POST methods, enter the data in the <b>POST data</b> box in the HTTP Settings section of the URL Sequence Step dialog box. For GET methods, enter the ACTION URL plus the &NAME=VALUE pairs in the <b>URL</b> box in the Reference Settings section of the URL Sequence Step dialog box. This requires familiarity with the script, the form structure, and CGI request headers.

The figure below illustrates several of the principles of constructing a URL Sequence monitor using regular expressions. The regular expression shown in the figure can be used to extract URLs from Javascript or other Web page content. As indicated, content matches for a given step are performed on the content returned for that step. The parentheses used in the regular expressions cause the value matched by the expression inside the parentheses to be remembered or retained. This retained value can be passed on to the next step of the sequence by using the { $n$ } variable. Because the regular expression can contain more than one set of parentheses, the  $n$  represents the match value from the  $n^{\text{th}}$  set of parentheses.



The example in the figure uses only one set of parentheses and thus references the retained value as `{$1}`.



Web pages containing code that perform the following present additional challenges:

- ▶ A script parses a cookie or other dynamic content to be added to a CGI GET request.
- ▶ Link information is contained in an external script file accessed by using a HTML `<SCRIPT HREF="http://... >` tag.

Web pages with dynamically generated link and form content may not be parsed correctly by the SiteScope URL Sequence monitor.

## Retaining and Passing Values Between Sequence Steps

One important function of the match content capability in URL Sequence monitor is the ability to match, retain, and then reference values from one URL sequence step for use as input in a subsequent step. Using one or more sets of parentheses as part of a match content regular expression instructs SiteScope to remember the values matched by the pattern inside the parentheses. These values can then be referenced using the syntax described in the following example.

### Example

Suppose you create a URL Sequence monitor and include a match content expression for the first step to capture some session information. The Step 1 match content expression could be in the form of

```
/[\w\s]*?(pattern1)[\/-=]*?(pattern2)/
```

The two sets of parentheses in this expression instruct SiteScope to retain the two values matched by `pattern1` and `pattern2`. To use these values as input to the **next** step in the URL sequence, use the syntax `{$valuenum}`. In this example, the string `{$1}` references the value matched by `pattern1` and `{$2}` references the value matched by `pattern2`. Use the above syntax for passing the referenced values to the URL sequence step immediately following the step in which the content match was made (step 1 to step 2 in our example).

You can retain and pass matched values from one step to any other subsequent step by using a compound syntax of `$$$stepnum.valuenum`. If, in our example, you want to use the value matched by `pattern1` in step 1 as input in a FORM or URL request in step 4 of the URL sequence, you would include the syntax `$$$1.1` in step 4. To reference the value matched by `pattern2`, use the `$$$1.2` syntax.

## Sharing Cookies Between Monitor Runs and Configured Monitors

The URL Sequence monitor also supports sharing cookies between monitor runs and between configured monitors. This is done by maintaining a persistency of both session cookies and permanent cookies that can be queried, updated and shared among other URL Sequence monitors.

Suppose you have a number of different URL Sequence monitors that are currently configured on a SiteScope server. Assume that all the monitors simulate a URL transaction in which at least one of the steps uses a session cookie to send to the server instead of logging in each time. Using cookie persistency, you can configure one monitor to save the cookies it receives and configure all the other monitors to load the cookies. This can save system costs if there is a charge for each request to the login server from the monitoring tool. The monitor can 'log in' once and reuse the credentials from the login by other monitor runs and monitor instances. Thus, only one monitor needs to contain a login step. All the others can skip this step and send the login credentials in a cookie instead.

**Note:**

- ▶ Configure the monitor designated to save cookies to run at a frequency that is not less than the time frame of the session to make sure that cookies remain valid throughout the time frame of a session. A monitor that loads cookies from the persistency file does not check to see whether the cookie it is loading and sending is still valid.
  - ▶ Configure the monitor designated to save cookies before you configure the loading monitors. This is to make sure that the persistency file exists when you configure monitors to load from the file. Configuring the saving monitor to run at a higher frequency than loading monitors does not assure that the monitor saving cookies runs first.
- 

## **Troubleshooting and Limitations**

You can run all the steps defined in the URL sequence by clicking the **Test Steps** button in the Step Settings panel. This displays the data collected from each step, and embeds a copy of the HTML page returned. For details, see “Step Settings” on page 1001.

## **Configuring the Monitor**

For task details, see “Create a URL Sequence” on page 997.

For user interface details, see “URL Sequence Monitor Settings” on page 1000.

## Create a URL Sequence

This task describes the steps and settings you use to create a URL sequence.

This task includes the following steps:

- “Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)” on page 997
- “Add a URL Sequence Monitor” on page 997
- “Start a New URL Sequence” on page 998
- “Define Additional Sequence Steps” on page 998
- “Enter an Encrypted or Unencrypted Password (if required)” on page 999
- “Configure Other Settings for the Monitor” on page 1000

### **1 Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)**

If the Web server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate. Use one of the following methods for importing server certificates:

- Import the server certificates using SiteScope Certificate Management. For details, see “Import Server Certificates Using Certificate Management” on page 1537.
- Import the server certificates manually. For details, see “Import Server Certificates Manually” on page 947.

### **2 Add a URL Sequence Monitor**

Add the URL Sequence monitor to a monitor group container and enter a name for the monitor instance in the General Settings panel.

For details on the General Settings panel, see “General Settings” on page 356.

### 3 Start a New URL Sequence

Configure the first URL in the sequence in the URL Sequence Step dialog box. The URL sequence must begin with an initial URL.

- a** In the Step Settings panel of the New URL Sequence Monitor dialog box, click the **New Step** button.
- b** In the URL Sequence Step dialog box, enter the initial URL address in the Reference Settings section. This URL should be the initial Web page that the user is expected to see or the access point for the web-based system you are going to monitor.
- c** Complete the other sequence step settings as necessary and click **OK**. Generally, the URL is sufficient for the first step of most URL sequences.
- d** In the Step Settings panel, click the **Test Steps** button to run all the defined steps in the URL Sequence and display the results of data collected. For details on the URL Sequence test, see “URL Sequence Steps Results Dialog Box” on page 1013.

For details on the URL Sequence Step dialog box, see “URL Sequence Step Dialog Box” on page 1007.

### 4 Define Additional Sequence Steps

Configure the individual steps for the URL sequence in the URL Sequence Step dialog box.

- a** In the URL Sequence Step Settings panel of the New URL Sequence Monitor dialog box, click the **New Step** button.
- b** Use the options in the Reference Settings section to select how SiteScope progresses from one step of a URL sequence to the next. The options are:
  - **URL**. To go to a URL manually.
  - **Link**. To follow a hyperlink.
  - **Form**. To select a form button.
  - **Frame**. To select a frame within a frameset.
  - **Refresh**. To follow a meta refresh redirection.

For details on the reference types, see “Defining Sequence Steps” on page 987.

- c Complete the other sequence step settings as necessary and click **OK**. For details on the user interface, see “URL Sequence Step Dialog Box” on page 1007.

## 5 Enter an Encrypted or Unencrypted Password (if required)

You can give an encrypted or unencrypted password to the URL monitor in the URL Sequence Step dialog box.

- ▶ To give an unencrypted password, enter the password in the **password=** line in the **POST data** text box. The password you enter is displayed in the text box.
- ▶ To give an encrypted password to the URL monitor form, type the string password in the **Post data password key** text box. Enter the password itself in the **Post data password value** text box. The password is encrypted.

### Example - Unencrypted Password

POST data:	<pre> {{2}signInForm}email= {{2}signInForm}newCustomer=registeredCusto mer {{2}signInForm}password=mypassword           </pre>
Post Data Password Key:	<input type="text"/>
Post Data Password Value:	<input type="text"/>

### Example - Encrypted Password

POST data:	<pre> {{2}signInForm}email= {{2}signInForm}newCustomer=registeredCusto mer {{2}signInForm}password=           </pre>
Post Data Password Key:	<input type="text" value="password"/>
Post Data Password Value:	<input type="text" value="*****"/>

## 6 Configure Other Settings for the Monitor

Edit the monitor configuration settings as required.

For details on the URL Sequence Monitor Settings, see “URL Sequence Monitor Settings” on page 1000.

## URL Sequence Monitor User Interface

**This section includes:**

- ▶ URL Sequence Monitor Settings on page 1000
- ▶ URL Sequence Step Dialog Box on page 1007
- ▶ URL Sequence Steps Results Dialog Box on page 1013
- ▶ URL Sequence Monitor Settings on page 1000
- ▶ URL Sequence Step Dialog Box on page 1007
- ▶ URL Sequence Steps Results Dialog Box on page 1013

## URL Sequence Monitor Settings







<b>Description</b>	The URL Sequence monitor simulates a user's actions across a series of Web pages and URLs. This is particularly useful for monitoring and testing multi-page e-commerce transactions and other interactive online applications.  Use this page to add the monitor or edit the monitor's properties.  <b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b> , and select the monitor from the New Monitor Page.
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.



<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>➤ “Create a URL Sequence” on page 997</li> <li>➤ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “URL Sequence Monitor Overview” on page 983</li> <li>➤ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Step Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click the <b>New Step</b> button to open the URL Sequence Step dialog box and define the URL sequence steps. For details on the user interface, see “URL Sequence Step Dialog Box” on page 1007.
	Click the <b>Edit Step</b> button to open the URL Sequence Step dialog box and edit the properties of an existing URL sequence step. For details on the user interface, see “URL Sequence Step Dialog Box” on page 1007.
	Click the <b>Delete Last Step</b> button to delete the last step in the URL sequence.
	Click the <b>Select All</b> button to select all listed URL sequence steps.
	Click the <b>Clear Selection</b> button to clear the selection.
	Click the <b>Test Steps</b> button to run the defined steps in the URL Sequence, and display the results of data collected. The response embeds a copy of the HTML received from the HTTP request. For details, see “URL Sequence Steps Results Dialog Box” on page 1013.
<b>Step</b>	The step number in the URL sequence.
<b>Reference Type</b>	The URL of the sequence step.
<b>Title</b>	The name of this step within the sequence monitor.

## URL Sequence Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>Timeout (seconds)</b>	<p>The number of seconds that the URL Sequence monitor should wait for the entire sequence to complete before timing-out. Once this time period passes, the URL Sequence monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 60 seconds</p>
<b>Timeout for each step</b>	<p>Select to use the value entered for the Timeout above as the timeout for each step of the sequence rather than for the entire transaction. If the step takes more than this time to complete, the URL Sequence monitor logs an error and reports an error status.</p> <p><b>Default value:</b> Not selected</p>
<b>Retries</b>	<p>Enter the number of times that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request for is a recoverable error.</p> <p><b>Default value:</b> 0</p>
<b>If error, resume at step</b>	<p>You use this option to specify a URL sequence step to run in the case that a URL Sequence results in an error. This is useful when a URL sequence involves a user or customer login which would result in problems if the sequence ended without logging out.</p> <p>Use the drop-down list to select a URL sequence step to jump to in the case that any step in the sequence returns an error.</p>
<b>Run resume step and remaining steps</b>	<p>If the <b>If error, resume at step</b> option is selected and run, selection of this option causes SiteScope to run that step and continue running the other, subsequent steps until it reaches the end of the sequence.</p> <p><b>Default value:</b> Not selected</p>



GUI Element	Description
<b>Show detailed measurements</b>	<p>Select this box if you want SiteScope to record a detailed breakdown of the process times involved in retrieving the requested URL. These include the following:</p> <ul style="list-style-type: none"> <li>▶ <b>DNS lookup time.</b> The time it takes to send a name resolution request to your DNS server until you get a reply.</li> <li>▶ <b>Connection time.</b> The time it takes to establish a TCP/IP/Socket connection to the Web server.</li> <li>▶ <b>Server response time.</b> The time after the request is sent until the first byte (rather first buffer full) of the page comes back.</li> <li>▶ <b>Download time.</b> The time it takes to download the entire page.</li> </ul> <p><b>Default value:</b> Not selected</p>
<b>HTTP Settings</b>	
<b>Request headers</b>	<p>The header request lines sent by the HTTP client to the server. Headers should be separated by a linebreak. The standard list of HTTP1.1 request headers can be found in <a href="http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14">http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14</a>.</p> <p><b>Note:</b> Although this field is optional, some Web pages behave unexpectedly when the request header is missing (such as performing endless redirects, providing wrong content, and so forth).</p>
<b>HTTP version</b>	<p>Select the HTTP version for SiteScope to use. Some systems may not be designed to accept HTTP 1.1 requests headers. If this is the case, select HTTP 1.0.</p> <p><b>Default value:</b> HTTP version 1.1</p>

GUI Element	Description
<b>Retrieve images</b>	<p>Select this box if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by <code>IMG</code>, <code>BODY</code> (from the background property), and <code>INPUT TYPE=IMAGE</code> HTML tags.</p> <p>Images that appear more than once in a page are only retrieved once.</p> <p><b>Note:</b> If this option is checked, each image referenced by the target URL contributes to the download time. However, if an image times out during the download process or has a problem during the download, that time is not added to the total download time.</p> <p><b>Default value:</b> Not selected</p>
<b>Retrieve frames</b>	<p>Select this box if you want SiteScope to retrieve the frames references in a frameset and count their retrieval time in the total time to download this page. Frames include those referenced by <code>FRAME</code> and <code>IFRAME</code> tags. If <b>Retrieve Images</b> is also checked, SiteScope attempts to retrieve all images in all frames.</p> <p><b>Note:</b> If this option is checked, each frame referenced by the target URL contributes to the download time. However, if a frame times out during the download process or has a problem during the download, that time is not added to the total download time.</p> <p><b>Default value:</b> Not selected</p>

GUI Element	Description
<b>Use WinInet</b>	<p>Select this option if you want to use WinInet as an alternative HTTP client for this monitor.</p> <p>Select this option to use WinInet instead of Apache when:</p> <ul style="list-style-type: none"> <li>▶ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates while Apache does not.</li> <li>▶ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.</li> </ul> <p><b>Default value:</b> Not selected (Apache is used)</p>
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	(Optional) A proxy server can be used to access the URLs in the sequence. Enter the domain name and port of an HTTP Proxy Server.
<b>Proxy server user name</b>	<p>If the proxy server requires a name and password to access the URLs in the sequence, enter the name here.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy server password</b>	<p>If the proxy server requires a name and password to access the URLs in the sequence, enter the password here.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy NTLM V2</b>	Select this option if the proxy server requires authentication using NTLM version 2.
<b>Authentication Settings</b>	
<b>NTLM V2</b>	<p>Select this option if the URL you are accessing requires authentication using NTLM version 2.</p> <p><b>Default value:</b> Not selected</p>

GUI Element	Description
<b>Accept untrusted certificates for HTTPS</b>	<p>If you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope does not have the required server certificates, you can either select this option or import the related certificates. For details on importing server certificates, see SSL Connectivity in “URL Sequence Monitor Overview” on page 983.</p> <p><b>Default value:</b> Not selected</p>
<b>Accept invalid certificates for HTTPS</b>	<p>Select this option if you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope has invalid server certificates. This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.</p> <p><b>Default value:</b> Not selected</p>
<b>Use cookie persistency</b>	<p>Select this option if you want to share cookies between monitor runs and between configured monitors. For details, see “Sharing Cookies Between Monitor Runs and Configured Monitors” on page 995.</p> <p><b>Default value:</b> Not selected</p>
<b>Load cookies from persistency</b>	<p>Select this option if you want to load all relevant cookies from the persistency file and add them to the list of cookies to be sent to the server. Cookies are loaded at the beginning of the monitor run.</p> <p><b>Default value:</b> Not selected</p>
<b>Save cookies to persistency</b>	<p>Select this option if you want to save all cookies received from the server for the current monitor run to the persistency file. Where a cookie has the same name, and its domain and path attribute string values exactly match those of an existing cookie in the persistency file, the cookie replaces the existing cookie. Cookies are saved at the end of every monitor run and the persistency file is updated.</p> <p><b>Default value:</b> Not selected</p>
<b>Cookie persistency file path</b>	<p>Enter the path and name of the cookie persistency file.</p>

## URL Sequence Step Dialog Box

<b>Description</b>	<p>Displays the settings used for each individual sequence step in the URL Sequence Step Settings panel of the New URL Sequence Monitor dialog box. The scope of each of these settings is limited to the request action for the step. For example, the <b>User name</b> and <b>Password</b> settings are only sent as part of the request being made in the step that they are defined.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the <b>URL Sequence</b> monitor. In the <b>Step Settings</b> panel, click the <b>New Step</b>  or <b>Edit Step</b>  button.</p>
<b>Included in Tasks</b>	“Create a URL Sequence” on page 997
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “URL Sequence Monitor Overview” on page 983</li> <li>➤ “URL Sequence Monitor Settings” on page 1000</li> <li>➤ “URL Sequence Steps Results Dialog Box” on page 1013</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Reference Settings</b>	
<Reference type>	<p>Use these options to select how SiteScope progresses from one step of a URL sequence to the next. For details, see “Defining Sequence Steps” on page 987.</p> <ul style="list-style-type: none"> <li>▶ <b>URL.</b> Go to a particular URL directly. Enter the URL you want SiteScope to go to in the URL box.</li> <li>▶ <b>Link.</b> Follow a hyperlink on the page received from the previous step. Click to display all available links on the current page. Click the label or HTML text corresponding to the hyperlink that you want SiteScope to follow. If you know a link is available on the subject page but it does not appear in the drop-down list, it may that the page uses a client-side program. In this case, you may have to specify the URL manually.</li> <li>▶ <b>Form.</b> Enter data into a form received from the previous step and submit the form data to an application. Click to display the list of available form buttons. Click the name or HTML text corresponding to the form button that you want SiteScope to use. If you know a form is available on the subject page but it does not appear in the drop-down list, see “URL Sequences and Dynamic Content” on page 990.</li> <li>▶ <b>Frame.</b> Request the content of a specific frame if the previous step returned an HTML frameset. Click the arrow on the right of the box to display all available filenames displayed in the current FRAMESET and then click the file that you want SiteScope to retrieve.</li> <li>▶ <b>Refresh.</b> Follow an automated redirection defined by a META HTTP-EQUIV="Refresh" tag. Click the arrow on the right of the box to display all available Refresh filenames, and select the file that you want SiteScope to retrieve. Normally there is only one filename.</li> </ul>
<b>Main Settings</b>	
<b>Step title</b>	Enter the text for the title of this step within the sequence monitor. The title is only displayed in the URL Sequence Steps Settings panel.




GUI Element	Description
<b>Match content</b>	<p>Enter a string of text to check for in the returned page or frameset. If the text is not contained in the page, the monitor displays the message content match error.</p> <p>HTML tags are part of a text document, so include them if they are part of the text for which you are searching. This works for XML pages as well.  <b>Example:</b> &lt; B&gt; Hello&lt; /B&gt; World</p> <p>You can also perform a regular expression match by enclosing the string in forward slashes, with a letter i after the trailing slash indicating case-insensitive matching.  <b>Example:</b> /href=Doc\d+\.html/ or /href=doc\d+\.html/i</p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression.  <b>Example:</b> /Temperature: (\d+). This returns the temperature as it appears on the page and this could be used when setting an <b>Error if</b> or <b>Warning if</b> threshold.</p> <p><b>Note:</b> The search is case sensitive.</p>
<b>Match content for error</b>	<p>Enter a string of text to check for in the returned page for this step. If the text is contained in the page, the monitor display the message <b>content error found</b> for this step's URL. The search is the same as for the <b>Match content</b> box described above.</p>
<b>Delay (seconds)</b>	<p>Enter how long SiteScope should wait before executing the next step of the sequence.</p> <p><b>Default value:</b> 0 seconds</p>
<b>Authentication Settings</b>	
<b>User name</b>	<p>If the URL specified for this step requires a name and password for access, enter the user name. Alternately, you can leave this entry blank and enter the user name in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.</p>

GUI Element	Description
<b>Password</b>	<p>If the URL specified for this step requires a name and password for access, enter the password. Alternately, you can leave this entry blank and enter the password in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.</p>
<b>Pre-emptive authorization</b>	<p>Select when the authorization credentials should be sent if SiteScope requests the target URL.</p> <ul style="list-style-type: none"> <li>▶ <b>Use global preference</b> (default value). Select to have SiteScope use the settings specified in the <b>Pre-emptive authorization</b> field in the Main Panel of the General Preferences page.</li> <li>▶ <b>Authenticate first request</b>. Select to send the user name and password on the first request SiteScope makes for the target URL. <b>Note:</b> If the URL does not require a user name and password, this option may cause the URL to fail.</li> <li>▶ <b>Authenticate if requested</b>. Select to send the user name and password on the second request if the server requests a user name and password. <b>Note:</b> If the URL does not require a user name and password, this option may be used.</li> </ul> <p>All options use the authorization <b>User name</b> and <b>Password</b> entered for this monitor instance. If these are not specified for the individual monitor, the <b>Default authentication user name</b> and <b>Default authentication password</b> specified in the Main Panel of the General Preferences page are used, if they have been specified.</p> <p><b>Note:</b> Pre-emptive authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
<b>Client side certificate</b>	<p>If you need to use a client side certificate to access the target URL, select the certificate file using the drop down menu. Client side certificate files must be copied into the <b>SiteScope\templates.certificates</b> directory. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You enter the password for the certificate in the <b>Client side certificate password</b> box.</p> <p><b>Default value:</b> none</p>

GUI Element	Description
<b>Client side certificate password</b>	If you are using a client side certificate and that certificate requires a password, enter the password.
<b>Authorization NTLM domain</b>	Enter the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL in this step.
<b>HTTP Settings</b>	
<b>URL content encoding</b>	SiteScope retrieves the correct encoding from the server response. The default value appearing here should not be edited. <b>Default value:</b> Retrieve encoding from server response
<b>POST data (for Form)</b>	<p>If the URL at this step issues a POST request for a form and the user has used the <b>Form</b> reference type (indicating that the user wants to send the form), enter the post variables, one per line as name=value pairs. This option is used to verify that a form is working correctly by performing the same request that occurs when a user manually submits a form. When the form is submitted, SiteScope fills in any items that are not specified with data here with the same defaults as a browser would have chosen.</p> <p>A single name=value pair may be used to hide any data that is passed to the form, such as a password. The values entered in the <b>POST data</b> text box are not encrypted and are visible to anyone. If you want to secure the value by encrypting it, use the <b>Post data password key</b> and <b>Post data password value</b> boxes to secure the monitor as described below.</p> <p><b>Note:</b> There may be more than one form on the page.</p>
<b>Post data password key</b>	Enter the name of the box that was supplied by the URL in the <b>POST data</b> box. It is the <b>name</b> component of the name=value pair.

GUI Element	Description
<b>Post data password value</b>	<p>Enter the value that is required when accessing the form. This is the <b>value</b> component of the name=value pair. The value is encrypted using the TDES algorithm.</p> <p>For example, you want to define an encrypted password to the form that the URL monitor, gmail.com sends. The site gmail.com automatically supplies information in the POST data text box of the URL Sequence dialog box. The Post Data Password Key may vary from site to site. The Post Data Password Key provided by gmail.com is Passwd. The Post Data Password Value is the password that you provide.</p> <p>For details on how to enter an encrypted or unencrypted password, see “Enter an Encrypted or Unencrypted Password (if required)” on page 999.</p>
<b>POST Data encoding</b>	<p>Determines if the Post Data is encoded. Select from the following options:</p> <ul style="list-style-type: none"> <li>▶ <b>Use content-type.</b> Decide to encode the post data by the content type header. If the header equals <b>urlencoded</b> then encode, otherwise do not encode.</li> <li>▶ <b>Force URL encoding.</b> Always encode the post data.</li> <li>▶ <b>Do not force URL encoding.</b> Do not encode the post data.</li> </ul>
<b>Show Source</b>	<p>Click to open a new browser window that displays the source code of the URL returned by the previous request. You can use this window to copy data, such as a session ID or form data, from the Web page for use in the current step. The HTML Source folding panel at the bottom of the step page can also be used to view the source of the Web page. However, some browsers do not support copying data from this panel.</p>
<b>Show HTML</b>	<p>Click to open a new browser window that displays the URL in a regular browser view. You can use this window to match the <b>Link</b> and <b>Form</b> data displayed in the URL Sequence Monitor step dialog form with the elements as displayed on the Web page.</p>

## URL Sequence Steps Results Dialog Box

<b>Description</b>	<p>Displays the data collected from running all the URL steps defined in the Step Settings panel. This includes the status and time taken for each step in the sequence. A copy of the HTML page returned at each step of the sequence is also displayed, so that a more graphical view of the sequence can be viewed.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the <b>URL Sequence</b> monitor. In the <b>Step Settings</b> panel, configure the individual steps for the URL sequence, and then click the <b>Test Steps</b>  button to view the test results.</p>
<b>Included in Tasks</b>	“Create a URL Sequence” on page 997
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “URL Sequence Monitor Overview” on page 983</li> <li>➤ “URL Sequence Step Dialog Box” on page 1007</li> <li>➤ “URL Sequence Steps Results Dialog Box” on page 1013</li> </ul>



# 94

---

## VMware Performance Monitor

This chapter includes the main concepts, tasks, and reference information for the VMware Performance monitor.

### **This chapter includes:**

#### **Concepts**

- ▶ VMware Performance Monitor Overview on page 1015

#### **Tasks**

- ▶ Configure the VMware Performance Monitoring Environment on page 1019
- ▶ Import the VMware Server Certificates on page 1020

#### **Reference**

- ▶ VMware Performance Monitor Settings on page 1021

### **VMware Performance Monitor Overview**

Use the VMware Performance monitor to monitor VMware-based servers. VMware supplies much of the virtualization software available for x86-compatible computers. The VMware Performance monitor supports monitoring:

- ▶ Single VMware ESX server installations.
- ▶ ESX server clusters managed by VMware Virtual Center.
- ▶ VMotion of virtual machines.

During initial monitor creation, the new monitor uses the connection URL configured to access the software and dynamically discover the object hierarchy and available performance counters. You can select from these performance counters to determine which measurements SiteScope should retrieve for reporting server status.

For details describing all the available counters, refer to the VMware documentation available at <http://www.vmware.com/pdf/ProgrammingGuide201.pdf>

This section contains the following topics:

- “Supported Versions” on page 1016
- “Setup Requirements” on page 1017
- “VMotion Support” on page 1017
- “SSL Connectivity” on page 1017
- “VMware Performance Topology Settings” on page 1018
- “Troubleshooting and Limitations” on page 1018
- “Configuring the Monitor” on page 1019

### **Supported Versions**

This monitor supports monitoring remote servers running on:

- VMware VirtualCenter 2.x
- VMware ESX 3.x
- VMware ESXi 3.5
- VMware ESX 2.5 via VirtualCenter 2.x
- VMware ESX 3.x via VirtualCenter 3.x



## Setup Requirements

The following are the requirements for monitoring VMware-based servers:

- ▶ The monitored VI server or ESX server cluster must be directly accessible by the SiteScope server (no proxy involved).
- ▶ The VI server or ESX server cluster provides connection either by http or by https (depending on the VI server configuration). If https is used, server certificate must be imported to the SiteScope.

## VMotion Support

VMware's VMotion technology enables transparent migration of running virtual machines between physical hosts in a virtual infrastructure cluster. It enables you to move an entire running virtual machine instantaneously from one server to another with continuous service availability and zero downtime. This process can be done both manually and automatically as part of cluster load balancing.

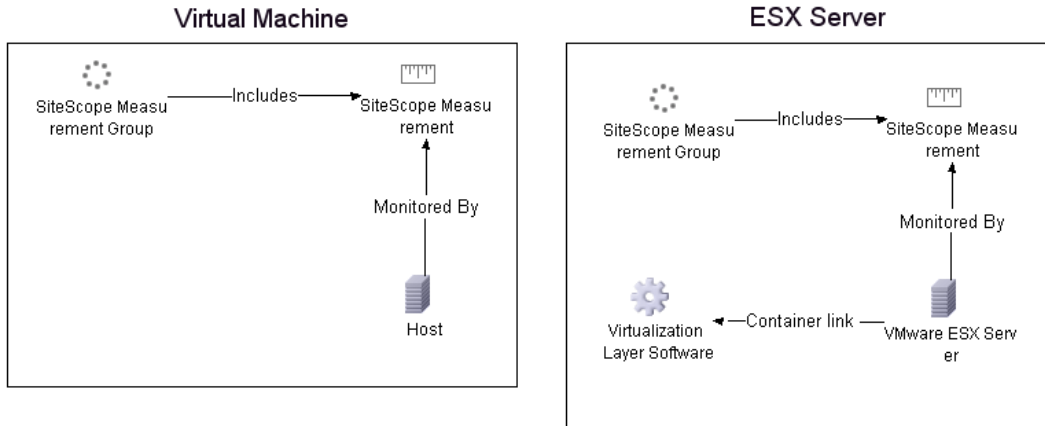
The VMware Performance monitor is browseable, and the counters tree is designed so that virtual machine nodes are not children of physical host nodes. This means that the structure of the tree does not change during migration and if counters from a virtual machine are selected for this monitor, they do not change as a result of VMotion. This is regardless of where the virtual machine belonged at any particular moment.

## SSL Connectivity

VMware servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The https:// prefix means that it is a secure, encrypted connection. Monitoring a VMware server which uses an encrypted connection, requires importing the server certificate. For details on how to perform this task, see "Import the VMware Server Certificates" on page 1020.

## VMware Performance Topology Settings

The VMware Performance monitor can identify the topology of the VMware servers being monitored. If **Include topology data when reporting to BAC** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160 in the HP Business Availability Center Documentation Library.

## Troubleshooting and Limitations

If you encounter errors retrieving the counters after upgrading from an earlier version of SiteScope, you should re-install the server certificate as follows:

- 1 Create a backup of the **cacerts** file in a directory outside of the SiteScope directory. The **cacerts** file is located in the `<SiteScope root directory>java\lib\security` folder.
- 2 Remove the **cacerts** file from the SiteScope folder.
- 3 Restart the SiteScope server.
- 4 Create a new **cacerts** file with the new certificate.

## Configuring the Monitor

For task details, see “Configure the VMware Performance Monitoring Environment” on page 1019.

For user interface details, see “VMware Performance Monitor Settings” on page 1021.

For details on managing server certificates, see “Certificate Management” on page 1535.

## Configure the VMware Performance Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Import the VMware Server Certificates” on page 1020
- “Configure the Monitor Properties” on page 1020

### **1 Import the Server Certificates (if the Web Server is Configured to Use SSL Encryption)**

If the Web server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate. Use one of the following methods for importing server certificates:

- Import the server certificates using SiteScope Certificate Management. For details, see “Import Server Certificates Using Certificate Management” on page 1537.
- Import the server certificates manually. For details, see “Import the VMware Server Certificates” on page 1020.

## 2 Configure the Monitor Properties

Complete the VMware Performance monitor configuration. For details on the monitor settings, see “VMware Performance Monitor Settings” on page 1021.

## Import the VMware Server Certificates

If the VMware server has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate. You can import the certificates manually using the `keytool` method.

---

**Tip:** Alternatively, you can import the server certificates without having to restart SiteScope by using Certificate Management. For details, see “Import Server Certificates Using Certificate Management” on page 1537.

---

### To import server certificates manually:

- 1 Export the certificate by going to the VMware administration URL and performing the export procedure described in the document.
- 2 Import the certificate, from the `<SiteScope root directory>java\lib\security`, by entering:

```
../../bin/keytool -import -file myCert.cer -alias myalias -keystore cacerts
```

Make sure to specify a unique alias for every certificate you add. If you do not, the `keytool` uses an automatic alias and once you attempt to add more than one custom certificate, the new certificate overwrites the old one and keeps only the default alias.

The word `changeit` is the default password for the `cacerts` file.

---

**Note:** The default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Therefore, you should create a copy of the **cacerts** file with a different name before SiteScope is upgraded or re-installed so that the file is not overwritten when new certificates are imported.

---

- 3 In SiteScope, select **Preferences > Certificate Management**, and click the **Reload Certificate List** button to reload the keystore certificates from the **cacerts** file. This enables you to manually reload keystore changes without having to restart SiteScope.

## VMware Performance Monitor Settings

<p><b>Description</b></p>	<p>The VMware Performance monitor enables you to monitor performance statistics of the VMware infrastructure for various server applications.</p> <p>The monitor supports monitoring both single VMware ESX server installations and ESX server clusters managed by VMware Virtual Centers.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>➤ Monitors must be created in a group in the monitor tree.</li> <li>➤ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>

<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>➤ “Configure the VMware Performance Monitoring Environment” on page 1019</li> <li>➤ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “VMware Performance Monitor Overview” on page 1015</li> <li>➤ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### VMware Performance Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>URL</b>	<p>Select the VMware infrastructure for the server you want to monitor.</p> <p>The format of the URL is:                      &lt;protocol&gt;://&lt;server_name&gt;/sdk                      where &lt;protocol&gt; is either http or https, and &lt;server_name&gt; is the name of the VI server.</p>
<b>User name</b>	The user name of the VMware Web service’s administrator.
<b>Password</b>	The password of the VMware Web service’s administrator.
<b>Socket timeout (milliseconds)</b>	<p>Enter the number in milliseconds that the VMware Performance monitor should wait for data from a server during a single data request. After the socket timeout period elapses, the monitor logs an error and reports the error status.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ The socket timeout value must be larger than 0.</li> <li>➤ The value of zero is interpreted as an infinite timeout.</li> </ul> <p><b>Default value:</b> 600000</p>

GUI Element	Description
<b>Counter Settings</b>	
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>





# 95

---

## Web Script Monitor

This chapter includes the main concepts, tasks, and reference information for the Web Script monitor.

### **This chapter includes:**

#### Concepts

- ▶ Web Script Monitor Overview on page 1026

#### Tasks

- ▶ Configure the Web Script Monitoring Environment on page 1035

#### Reference

- ▶ Web Script Monitor Settings on page 1037

## Web Script Monitor Overview

The Web Script monitor proactively monitors Web sites in real time, identifying performance problems before users experience them. It enables you to monitor sites from various location where SiteScope is installed, emulating the end-user experience. You can assess site performance from different client perspectives.

---

### Note:

- ▶ The Web Script monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
  - ▶ This monitor is supported in SiteScopes that are running on Windows versions only.
  - ▶ The Web Script monitor is not supported in template mode.
- 

The Web Script monitor runs the scripts created in the HP Virtual User Generator (VuGen). You use VuGen to create a script that emulates end-user actions. You can create the script with the steps that you want monitored on target Web sites. For information on working with VuGen, see “Working with VuGen” on page 1031.

---

**Note to HP Business Availability Center users:** The Web Script monitor is not available when working in HP Business Availability Center. The monitor’s data cannot be reported to HP Business Availability Center.

---

This section contains the following topics:

- “What to Monitor” on page 1027
- “Counter Measurements and Transaction Breakdown Data” on page 1027
- “Setting up the Web Script Monitor” on page 1028
- “Selecting Counters” on page 1028
- “Advanced Information” on page 1029
- “Troubleshooting and Limitations” on page 1030
- “Configuring the Monitor” on page 1030

## **What to Monitor**

You can create transactions to monitor pages that are critical to your Web applications, pages that are generated dynamically, and pages that depend on other applications to work correctly (such as pages that utilize a back-end database).

## **Counter Measurements and Transaction Breakdown Data**

Each time the Web Script monitor runs the VuGen script, it returns the transaction breakdown and performance data. The VuGen script also includes content match functionality, enabling you to check images, texts, links, and other areas of the Web site.

In addition, the monitor’s reported data can include the following measurements:

- The amount of time needed to establish an initial connection with the Web server performing the transaction.
- The amount of time taken to establish an SSL connection for HTTPS connections.
- The time in milliseconds for the transaction to be run.
- Whether the transaction passed or failed to connect and perform its required steps.

- ▶ Number of pages accessed when running the transaction.
- ▶ Number of errors that occurred during the transaction run.

The monitor can provide early indicators of the following performance issues:

- ▶ Excessive connection or retry times.
- ▶ Slow DNS resolution or other problems with the DNS server.
- ▶ Problems along the network or whether the server is responsive to requests.
- ▶ Delays or failures in secured or authorized connections.
- ▶ Overall network quality.
- ▶ Web server delays.

Each of the measurements is available as a parameter for assigning thresholds. This means that thresholds can be set for specific transactions and measurements, providing status indicators per transaction.

For details on selecting measurement counters, see “Selecting Counters” on page 1028.

## **Setting up the Web Script Monitor**

Prior to configuring the Web Script monitor in SiteScope, you must create the script in VuGen. The monitor runs only those scripts created in VuGen. For information on working with VuGen, see “Working with VuGen” on page 1031.

For an overview of the steps necessary to set up the Web Script monitor, see “Configure the Web Script Monitoring Environment” on page 1035.

## **Selecting Counters**

The Web Script monitor makes use of performance counters to measure Web sites performance. Select the counter metrics you want to monitor with the Web Script monitor. For details on adding performance counter metrics, see “Web Script Monitor Settings” on page 1037. For details on the counter metrics available for the monitor, see “Web Script Performance Counters” on page 1040.

## Advanced Information

The Web Script monitor uses an internal engine to run the VuGen scripts you create. This section includes some advanced issues.

SiteScope makes a copy of the script created in VuGen and stores it in a location within the SiteScope directory. SiteScope makes the necessary modifications for the script to be run properly by the Web Script monitor. These modifications are automatic and cannot be manually duplicated. They include:

- ▶ Disabling the **Download Snapshots** operation.
- ▶ Disabling the **Think Time** operation.
- ▶ Disabling the **Iterations** operation.

Therefore:

- ▶ If there is any change made to the script in VuGen, including the name of the script, and you want the Web Script monitor to run the revised version of the script, you must edit the monitor in SiteScope and select the edited script in its saved location.
- ▶ Each script must have a unique name even if the different zip files for the scripts reside in different directories.
- ▶ The name of the zip file selected for the monitor must be the same as the name of the script created in VuGen.

## Troubleshooting and Limitations

This section includes troubleshooting issues for the Web Script monitor.

- ▶ Each time the monitor is run, a log is created. You can view the log to troubleshoot the monitor if you see there is a problem running the scripts. The logs are stored in `<SiteScope root directory>\cache\temp\WebScript\<name of script>\log`. You can search for the required log based on the name of the script run by the monitor and the time the log was created.

This directory is cleaned out every time SiteScope is restarted, which is every 24 hours by default.

- ▶ If the log files do not give you the necessary information to determine why the script is not running properly, run the script in VuGen. For details, refer to "Running Vuser Scripts in Standalone Mode" in the VuGen guide.
- ▶ If all the transaction breakdown counters for the monitor are reporting a status of -1 and there is a reported time for the Duration counter (the total running time of the transaction), it could be because the transaction breakdown times exceed the total running time. This can occur in rare cases because of the way the transaction breakdown times are calculated and because the Duration is an actual measurement of the total transaction time from start to finish, with no additional calculations. If the problem persists for a specific transaction, we recommend that you adjust the counters selected for the transaction.
- ▶ If you get the message "Error: Fail to get performance data timeout (error)" during the monitor run, add `LogFileWrite=1` to the **default.cfg** file of the specific script file to get more details about the error. If the script log shows that some of the resources are taking more time than the monitor timeout, increase the **Web script timeout (sec)** value in the monitor settings.
- ▶ The Web Script monitor supports script names with English characters only.

## Configuring the Monitor

For task details, see "Configure the Web Script Monitoring Environment" on page 1035.

For user interface details, see "Web Script Monitor Settings" on page 1037.

## Working with VuGen

VuGen can be used to automatically create a transaction script by recording the actual business processes and actions performed by users interacting with a Web application. VuGen captures all end-user activity between the client and the server, thereby capturing the exact tasks and functions users perform.

---

**Note:** The Web Script monitor supports scripts created in HP Virtual User Generator version 9.1 and earlier.

---

This section includes:

- “Getting Started” on page 1031
- “Supported VuGen Protocols” on page 1032
- “Inserting Transactions and Creating Checkpoints” on page 1033
- “Saving and Storing the Script” on page 1034

### Getting Started

The VuGen help is accessible from the VuGen product once it is downloaded. It can be accessed in the following ways:

- Press F1 for context-sensitive help when working with a specific function.
- Select **Help > Contents and Index > Contents** tab > **Books Online > VuGen** to view the entire online guide. Use this option when searching for a specific topic referred to in the description of this monitor.
- Select **Help > Books Online > HP Virtual User Generator User’s Guide** to access the guide in PDF format.

The VuGen interface includes a detailed workflow that takes the user through the step-by-step process of creating a script. For information about the workflow, refer to "Working with VuGen" > "Viewing the VuGen Workflow" in the VuGen guide.

For more detailed information on creating scripts, refer to "Working with VuGen" > "Recording with VuGen" > "Creating New Virtual User Scripts" in the VuGen guide.

### **Supported VuGen Protocols**

The following are the protocols supported for the Web Script monitor.

- "Web (Click and Script) Protocol" on page 1032
- "Web (HTTP/HTML) Protocol" on page 1033

### **Web (Click and Script) Protocol**

This is the recommended protocol to use to record scripts to be run by the Web Script monitor.

Web (Click and Script) is a new approach to Web scripting. It introduces a GUI-level scripting API, and a quicker way to create scripts.

- Easy-to-use scripting.
- Intuitive API functions describe user actions on Web objects (for example, button and text link).
- In tree view, the steps are grouped according to their pages.
- In snapshot viewer, the object corresponding to the active step is highlighted.

For details on using this protocol, refer to the "Creating Web Vuser Scripts" and "Working with Web (Click and Script) Vuser Scripts" sections under "E-Business Protocols" in the VuGen guide.

### **Web (Click and Script) Limitations**

- Records and emulates on Internet Explorer version 6 only.
- Does not support recording on Microsoft Windows 2003.
- Does not support VBScript and applets.
- Does not support user actions on ActiveX objects and Macromedia Flash.
- Supports only English language applications.



---

**Note:** If any of these limitations affect your ability to record a script, use VuGen's Web (HTTP/HTML) Protocol instead. For details, see below. For information about choosing a protocol, refer to "E-Business Protocols" > "Choosing a Web Vuser Type" in the VuGen guide.

---

### **Web (HTTP/HTML) Protocol**

This is the standard VuGen protocol for recording Web applications.

When recording a Web (HTTP/HTML) script, VuGen records the HTTP traffic and server response over the Internet. The scripts contain detailed information about your actions in the browser.

The Web (HTTP/HTML) Vuser provides two recording levels: HTML-based script and URL-based script. These levels let you specify what information to record and which functions to use when generating a Vuser script.

For details on using this protocol, refer to the "E-Business Protocols" > "Creating Web Vuser Scripts" in the VuGen guide.

### **Inserting Transactions and Creating Checkpoints**

- ▶ While creating your VuGen script, you must insert transactions into the script. These transactions provide the breakdown performance data reported by the monitor.

For details on transactions, refer to "Working with VuGen" > "Enhancing Vuser Scripts" > "Inserting Transactions into a Vuser Script" in the VuGen guide.

- ▶ VuGen's Content Check mechanism enables you to check the contents of a page for a specific string. This is useful for detecting non-standard errors. We recommend that you include content check checkpoints in your script.

For details on checkpoints, refer to the "Checking Web Page Content" and "Verifying Web Pages under Load" sections under "E-Business Protocols" in the VuGen guide.

## Saving and Storing the Script

The script you create in VuGen must be saved as a zip file. We recommend saving only the runtime files. For details, refer to the "Recording with VuGen" and "Using Zip Files" sections of the VuGen guide.

When saving the zip file:

- make sure that the zip file has the same name as the script
- make sure that each script used for a Web Script monitor has a unique name

You can save the script into:

- The configured default location for VuGen scripts within the SiteScope root directory is **<SiteScope root directory>\templates.webscripts\**. This directory is automatically created.

By default, all the scripts in this directory appear in the drop-down list of available scripts when configuring the monitor.

- A different location for VuGen scripts that you configure in SiteScope's General Preferences.

You can change the default location of VuGen scripts by entering a value in the **VuGen scripts path route** box in General Preferences (**Preferences > General Preferences > Main Panel**). The scripts stored in the location you enter appear in the drop-down list of available scripts when configuring the monitor.

- Any other location accessible to the SiteScope machine.

When configuring the monitor, you can also enter the full directory path and name of the script. The Web Script monitor can access the script if the machine on which SiteScope is running has file system access to the path location.

## Configure the Web Script Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Create a Script Using HP Virtual User Generator (VuGen)” on page 1035
- “Create the Web Script Monitor in SiteScope” on page 1036

### 1 Create a Script Using HP Virtual User Generator (VuGen)

Prior to configuring the Web Script monitor in SiteScope, you must create the script in VuGen.

#### a Download HP Virtual User Generator (VuGen).

Go to the HP Software Support site (<http://www.hp.com/go/hpsupport>) and in the **Where do I find** section, click **Software patches**. In the **Product** section, select **SiteScope** and type **VuGen** in the optional search box. Download the required version of VuGen from the results. You must log in with your HP user name and password to access the Software Patches page.

To enable monitoring, you must also download the latest HP Virtual User Generator Feature Pack.

#### b Familiarize yourself with how to create scripts.

The script you create in VuGen is run by the Web Script monitor and must contain transactions. The VuGen interface contains different access points for getting help. For details, see “Getting Started” on page 1031.

#### c Use the supported protocols in Virtual User Generator to create your script.

---

**Tip:** We recommend that you use the Web (Click and Script) protocol to create your script for use in SiteScope. For a list of all the supported protocols and for details on the Web (Click and Script) protocol, see “Supported VuGen Protocols” on page 1032.

---

- d** Include transactions and content match checkpoints in your script.

The VuGen script must contain transactions to be run by the Web Script monitor in SiteScope. These transactions provide the breakdown performance data reported by the monitor. For details on transactions, refer to "Working with VuGen" > "Enhancing Vuser Scripts" > "Inserting Transactions into a Vuser Script" in the VuGen guide.

Checkpoints are recommended for checking contents of a page for a specific string while running the VuGen script. This is useful for detecting non-standard errors. For details on checkpoints, refer to the "Checking Web Page Content" and "Verifying Web Pages under Load" sections under "E-Business Protocols" in the VuGen guide.

- e** Save the script's runtime files into a zip file and save the zip file into the required directory.

For details, see "Saving and Storing the Script" on page 1034.

- f** Make sure that the script runs properly in VuGen before continuing.

For details, refer to "Working with VuGen" > "Running Vuser Scripts in Standalone Mode" in the VuGen guide.

## **2 Create the Web Script Monitor in SiteScope**

Add the monitor, and complete the monitor configuration. For details on the monitor settings, see "Web Script Monitor Settings" on page 1037.



## Web Script Monitor Settings

<b>Description</b>	<p>The Web Script monitor gives you a flexible solution for virtual end-user monitoring of all your Web-based Applications. It can monitor dynamic content, test various authentication methods, and capture each step in a transaction between virtual user and Web site. This can help identify performance and availability issues before they affect end users.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The Web Script monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.</li> <li>▶ The Web Script monitor is not supported in template mode.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ <b>Note to HP Business Availability Center users:</b> The Web Script monitor is not available when working in HP Business Availability Center and cannot be configured in System Availability Management. The monitor's data cannot be reported to HP Business Availability Center.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the Web Script Monitoring Environment” on page 1035</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Web Script Monitor Overview” on page 1026</li> <li>▶ “Web Script Performance Counters” on page 1040</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Web Script Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Web script URL</b>	<p>Select from the following options:</p> <ul style="list-style-type: none"> <li>▶ <b>Web script files list.</b> Select from the list of available scripts in the directory storing your VuGen scripts. This could be the default directory <code>&lt;SiteScope root directory&gt;\templates.webscripts</code> or a directory you name in <b>VuGen scripts path root</b> in General Preferences. For details, see “General Preferences User Interface” on page 1379.</li> <li>▶ <b>Full path Web script name.</b> Enter the full path for the VuGen script. The script must be a .zip file and the path must be a location to which the machine running SiteScope has file system access.</li> </ul> <p>When the script is selected, it is copied into a SiteScope directory and the monitor no longer accesses the original location or the original script files.</p> <ul style="list-style-type: none"> <li>▶ If the script is changed in VuGen and you want the monitor to run the newer version of the script, you must edit the monitor and select the script again.</li> <li>▶ Each script used for a Web Script monitor must have a unique name.</li> </ul>
<b>Web script timeout (seconds)</b>	<p>Enter the time in seconds after which you want SiteScope to stop running the script if it has not successfully completed its run.</p> <p>This value must be less than the value you entered for the Frequency setting.</p> <p><b>Default value:</b> 60 seconds</p>

GUI Element	Description
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor. For the list of counters available for the monitor, see “Web Script Performance Counters” on page 1040.</p> <p>The first list of counters applies to all the transactions in the script and is called <b>Total</b>. The <b>Status</b> counter is the only counter that is in the <b>Total</b> list and the only counter that can be applied to all the transactions within the script. The subsequent lists are by transaction. Each transaction list includes all the available counters, enabling you to make specific selections of counters for the different transactions in the script.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ Not all counters return values for all transactions.</li> <li>➤ When working in template mode, the maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</li> </ul>

## Web Script Performance Counters

The following table lists all the counter metrics available for the monitor. Not all the counters report on all the transactions.

Name	Description
<b>Retry Time</b>	<p>Displays the overall amount of time that passes from the moment an HTTP request is started until the moment an HTTP or TCP error message is returned.</p> <p>Retry time only relates to HTTP or TCP errors that execute a retry after the error.</p>
<b>DNS Time</b>	<p>Displays the average amount of time needed to resolve the DNS name to an IP address, using the closest DNS server.</p> <p>The DNS Lookup measurement is a good indicator of slow DNS resolution or other problems with the DNS server.</p>
<b>Connection Time</b>	<p>Displays the amount of time needed to establish an initial connection with the Web server performing the transaction.</p> <p>The connection measurement is a good indicator of problems along the network or whether the server is responsive to requests.</p>
<b>SSL Handshaking Time</b>	<p>Displays the amount of time taken to establish an SSL connection (includes the client hello, server hello, client public key transfer, server certificate transfer, and other optional stages). After this point, all the communication between the client and server is encrypted.</p> <p>The SSL handshaking measurement is only applicable for HTTPS communications.</p>
<b>Network Time to First Buffer</b>	<p>Displays the amount of time that passes from the moment the first HTTP request is sent until receipt of ACK.</p> <p>The network measurement is a good indicator of network quality (look at the time/size ratio to calculate download rate).</p>



Name	Description
<b>Server Time to First Buffer</b>	<p>Displays the amount of time that passes from the receipt of ACK of the initial HTTP request (usually GET) until the first buffer is successfully received back from the Web server. The server time to first buffer measurement is a good indicator of Web server delay.</p> <p><b>Note:</b> Because server time to first buffer is being measured from the client, network time may influence this measurement if there is a change in network performance from the time the initial HTTP request is sent until the time the first buffer is sent.</p>
<b>Download Time</b>	<p>Displays the time from the receipt of the first buffer until the last byte arrives.</p> <p>Download time is a combination of server and network time, because each server (as specified by the URLs in the script) sends data over two or four connections, and therefore is usually working while data is being transmitted over the network.</p> <p>As a Web page is retrieved, its various components (images, applets, and so on) travel in data packets from server to client across the connections, so that some data packets may be traveling over the network through one of the connections, while others are being processed by the server through another connection.</p>
<b>Client Time</b>	Displays the time during the script run when the client is not sending or receiving data from the server.
<b>Duration</b>	The time in milliseconds for the transaction to be run.
<b>Status</b>	Displays whether the transaction passed or failed. A value of 0 is passed, a value of 1 is failed. A failed transaction could be caused by a content matching error, as set up in the VuGen script, or an http error from the server.
<b>Size</b>	The size in bytes received from the Web sites being monitored by the transaction.
<b>Number of Errors</b>	Number of errors that occurred during the transaction run.
<b>Number of Pages</b>	Number of pages accessed when running the transaction.



# 96

---

## Web Server Monitor

This chapter includes the main concepts and reference information for the Web Server monitor.

### **This chapter includes:**

#### Concepts

- ▶ Web Server Monitor Overview on page 1043

#### Reference

- ▶ Web Server Monitor Settings on page 1044

### **Web Server Monitor Overview**

The Web Server monitor gathers information about a Web Server by reading the server log files. Using this information, you can see how busy your Web site is, and plan hardware upgrades and configuration changes to improve performance.

It is most effective if you create a separate Web Server monitor for each Web server you are running. If you are running multiple Web servers, each one should have its own log file so that SiteScope can report on them separately. For information about what data is recorded, see “SiteScope Log File Columns” on page 1932.

For details on configuring the monitor, see “Web Server Monitor Settings” on page 1044.

 **Web Server Monitor Settings**

<b>Description</b>	<p>The Web Server monitor reports information about a Web server by reading the server log files. Each time the Web Server monitor runs, it writes the current hits per minute and bytes per minute in the monitor status string and in the SiteScope logs.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the <b>Browse Servers</b> and <b>Add Remote Server</b> buttons are not displayed.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Web Server Monitor Overview” on page 1043</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Web Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>The server where the Web server instance you want to monitor is running. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope are displayed). Alternatively, click the <b>Browse Servers</b> button to select a server from the local domain, or <b>Add Remote Server</b> to add a new server.</p> <p><b>Note:</b> If SiteScope is installed on a Windows platform, this monitor can monitor a target Windows server that has a Web Server installed on it. If SiteScope is installed on a UNIX platform, this monitor can monitor local log files only (monitoring a Web Server on UNIX platforms is no longer supported).</p> <p><b>Note when working in template mode:</b> You can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</p> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

GUI Element	Description
<b>Browse Servers</b>	<p>Click to open the Select Server dialog box, and select the server to be monitored:</p> <ul style="list-style-type: none"> <li>▶ <b>Browse servers.</b> Select a server from the drop-down list of Windows servers visible in the local domain.</li> <li>▶ <b>Enter server name.</b> If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ This button is available for SiteScope running on Windows platforms only.</li> <li>▶ To monitor a remote Windows server, you must have domain privileges or authenticated access to the remote server. For details on how to configure a remote Windows server, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.</li> </ul>
<b>Add Remote Server</b>	<p>Click to open the Add Microsoft Windows Remote Server dialog box, and enter the configuration details. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</p> <p><b>Note:</b> This button is available for SiteScope running on Windows platforms only.</p>
<b>Web server</b>	<p>Select a Web server type for the selected Web server from the list of accessible server types.</p> <p><b>Default value:</b> Microsoft IIS</p> <p><b>Note:</b> This field is available for SiteScope running on Windows platforms only.</p>

GUI Element	Description
<b>Log file path</b>	<p>For SiteScope running on UNIX platforms: To monitor Web server statistics, enter the full path of the Web server log file.</p> <p>For SiteScope running on Windows platforms: If your Web server does not appear in the Web Server list, you may still monitor it by entering the full path to the Web server log file.</p> <p><b>Example:</b> <code>c:/ns-home/httpd-test/logs/access</code></p> <p>For servers that dynamically create the filename for log files, you can include regular expression as part of the log file path definition. The SiteScope can then retrieve data from a range of filenames based on evaluation of the regular expressions.</p>
<b>Request size column</b>	<p>If your Web server saves information in a custom format. Enter the column number which contains the Request Size.</p> <p>If this item is blank, the common log file format is assumed.</p>





# 97

---

## Web Service Monitor

This chapter includes the main concepts and reference information for the Web Service monitor.

**This chapter includes:**

**Concepts**

- ▶ Web Service Monitor Overview on page 1050

**Reference**

- ▶ Web Service Monitor Settings on page 1055

## Web Service Monitor Overview

Use the Web Service monitor to check the availability of a Web service accepting Simple Object Access Protocol (SOAP) requests. The Web Service monitor checks that the service can send a response to the client in certain amount of time and to verify that the SOAP response is correct based on your selected match specifications.

The Simple Object Access Protocol is a way for a program running under one operating system to communicate with another program running under the same or different operating system (such as a Windows 2000 program talking to a Linux based program) The Simple Object Access Protocol uses the Hypertext Transfer Protocol (HTTP) and Extensible Markup Language (XML) for information exchange with services in a distributed environment.

This monitor uses a Web Services Description Language (WSDL) file to extract technical interface details about a Web service and uses information returned to create an actual SOAP request to that Web service. That is this monitor emulates a real Web service client making a request. The SOAP request can be used to confirm that the Web service is serving the expected response data and in a timely manner. The status of the Web Service monitor is set based on the results of the SOAP request.

For information about SOAP, refer to the W3C Web site (<http://www.w3.org/TR/SOAP/>).

For information about WSDL, refer to the Microsoft site (<http://msdn2.microsoft.com/en-us/library/ms996486.aspx>).

This section contains the following topics:

- ▶ “Supported Technologies” on page 1051
- ▶ “Status” on page 1051
- ▶ “Integration with HP Business Availability Center for SOA” on page 1053
- ▶ “Web Service Topology Settings” on page 1053
- ▶ “Configuring the Monitor” on page 1054

## Supported Technologies

The following specification features are currently supported:

- WSDL 1.2
- SOAP 1.1 only (SOAP 1.2 is not supported)
- Simple and Complex Types based on XML Schema 2001
- SOAP binding with the HTTP(S) protocol only
- SOAP with Attachments is not supported
- Nested WSDL
- WSDL with multi-ports and multi-services

---

**Note:** SOAP and WSDL technologies are evolving. As a result, some WSDL documents may not parse accurately and some SOAP requests may not interact with all Web service providers. When SiteScope is unable to generate the correct skeleton code, for example, if the WSDL file has errors or the complexType element uses schema syntax that is not supported, you can modify the XML argument as necessary. For example, if an argument is displayed like this:

```
parameters[COMPLEX] =<pPatientSSN xsi:type="xs:string">***</pPatientSSN>
```

you can modify it by deleting the **xs:** and **xsi:** as follows:

```
parameters[COMPLEX] =<pPatientSSN type="string">***</pPatientSSN>
```

---

## Status

The status reading shows the most recent result for the monitor. It is also recorded in the SiteScope log files, email alert messages, and can be transmitted as a pager alert. The possible status values are:

- OK
- unknown host name
- unable to reach server

- unable to connect to server
- timed out reading
- content match error
- document moved
- unauthorized
- forbidden
- not found
- proxy authentication required
- server error
- not implemented
- server busy

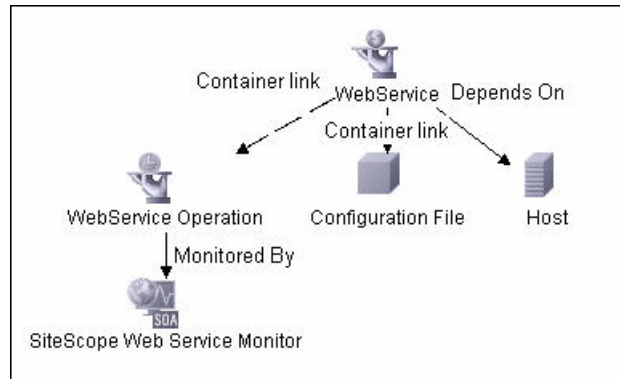
The final status result is either OK, error, or warning based on the threshold established for these conditions.

## Integration with HP Business Availability Center for SOA

If SiteScope is reporting to HP Business Availability Center, the monitor sends SOA samples, in addition to the regular samples it sends, for use in HP Business Availability Center for SOA. If the logging setting in **HP BAC Integration Settings** is set to **Disable reporting to BAC**, the monitor does not send any samples to HP Business Availability Center.

## Web Service Topology Settings

The Web Service monitor can identify the topology of the Web Service being monitored. If **Include topology data when reporting to BAC** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



The CIs are created only for the monitored entities according to the counters that you select.

**Note:**

- ▶ This direct integration between SiteScope and Business Availability Center is available only when the Business Availability Center for SOA license is installed.
  - ▶ The SiteScope Web Service Monitor CI replaces the legacy SiteScope Monitor CI for the Web Service monitor instances when upgrading from previous versions of SiteScope to SiteScope 9.50. The SiteScope Monitor CI is removed from CMDB, which causes it to be removed from views that included it or from SLAs to which it was attached.
- 

For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160.

For information about the SOA topology, see “SOA Views and Their Components” in *Solutions and Integrations* in the HP Business Availability Center Documentation Library.

### **Configuring the Monitor**

For details on configuring the monitor, see “Web Service Monitor Settings” on page 1055.

 **Web Service Monitor Settings**

<b>Description</b>	<p>The Web Service monitor is used to check Simple Object Access Protocol (SOAP) enabled Web services for availability and stability. The Web Service monitor sends a SOAP based request to the server and checks the response to verify that the service is responding.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>Web Service Tool</b> is available when configuring this monitor to test the availability of SOAP enabled Web Services (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Web Service Tool” on page 251.</li> </ul>
<b>Included in Tasks</b>	“Deploy a Monitor – Workflow” on page 323
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Web Service Monitor Overview” on page 1050</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Web Service Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>WSDL Settings</b>	
<b>WSDL location</b>	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>▶ <b>File.</b> Select the WSDL file to be used for this monitor. This list reflects the files found by searching on <b>&lt;SiteScope root directory&gt;\templates.wSDL/*.wsdl</b>.</li> <li>▶ <b>URL.</b> Enter the URL of the WSDL file to be used for this monitor.</li> </ul> <p>Your WSDL files must have the extension <b>.wsdl</b>.</p>
<b>Get Data</b>	<p>Clicking the <b>Get Data</b> button causes the specified WSDL file to be retrieved and analyzed for method arguments. The ensuing page displays the measurements available for monitoring.</p>
<b>Service name</b>	<p>Select the name of the service to be invoked. During initial setup, this is extracted from the WSDL file.</p>
<b>Port name</b>	<p>Select the name of the port to be invoked. During initial setup, this is extracted from the WSDL file.</p>
<b>Method name</b>	<p>Select the name of the method to be invoked. During initial setup, this is extracted from the WSDL file.</p>
<b>Method name space</b>	<p>The XML name space for the method in the SOAP request. During initial setup, this value is extracted from the WSDL file.</p>
<b>Schema name space</b>	<p>The XML name space for the schema in the SOAP request. During initial setup, this value is extracted from the WSDL file.</p>
<b>SOAP action</b>	<p>The SOAP action URL in the header of the SOAP request to the Web Service. During initial setup, this is extracted from the WSDL file.</p>



GUI Element	Description
<b>Name of arguments</b>	<p>Shows the name and type/structure of the arguments to the method specified above. SiteScope supports both simple (primitive) and complex (user-defined using XML schema) types.</p> <p>Simple type arguments appear in the form:  parm-name(parm-type) =  where you need to enter the parameter value to be used in invoking the Web service after the equal sign. Strings with embedded spaces should be enclosed in double quotes. Each parameter must be in a separate line, that is, do not remove the carriage return at the end of each parameter.</p> <p>A complex type parameter is displayed as one long string, with needed input fields marked with asterisks (**). An example of a complex type parameter is shown below:</p> <pre>stocksymbol[COMPLEX] =&lt;stocksymbol xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fw100="urn:ws-stock" xsi:type="fw100:getQuote"&gt; &lt;ticker xsi:type="xsd:string"&gt;***&lt;/ticker&gt;&lt;/stocksymbol&gt;</pre> <p>You must replace these occurrences of asterisks with meaningful values of the required type (in the example above, xsd:string), otherwise the Web service request may fail. Do not add any carriage returns within a complex type parameter.</p> <p>If the Web service method does not take any parameters, the text box must be empty.</p> <p><b>Note:</b> SiteScope cannot set the order of arguments. If the order is important, enter arguments in the same order in which they appear in the WSDL file.</p>
<b>Use user-defined SOAP XML</b>	<p>Select this check box to use the XML in the <b>Use SOAP XML</b> box. This enables you to use XML that has been manually defined.</p>

GUI Element	Description
<b>Use SOAP XML</b>	Displays the SOAP XML for the selected Web service extracted from the WSDL file. You can make changes to the default XML, and use the manually defined XML in this box by selecting the <b>Use User-Defined SOAP XML</b> check box.
<b>Main Settings</b>	
<b>Request's schema</b>	The request schema. Currently SiteScope only supports SOAP.
<b>Timeout (seconds)</b>	Enter the total time, in seconds, that SiteScope should wait for the Web service request to complete. <b>Default value:</b> 5 seconds
<b>Use .NET SOAP</b>	Select this check box if the Web service is based on Microsoft .NET.
<b>Content match</b>	<p>Enter a string of text to check for in the returned page or frameset. If the text is not contained in the page, the monitor displays the message no match on content.</p> <p>HTML tags are part of a text document, so include the HTML tags if they are part of the text you are searching for. This works for XML pages as well. <b>Example:</b> "&lt; B&gt; Hello&lt; /B&gt; World"</p> <p>You may also perform a regular expression match by enclosing the string in forward slashes, with an <i>i</i> after the trailing slash to indicate that the search is not case sensitive. <b>Example:</b> <code>/href=Doc\d+\.\html/</code> or <code>/href=doc\d+\.\html/i</code></p> <p>If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a Perl regular expression. <b>Example:</b> <code>/Temperature: (\d+)</code></p> <p><b>Note:</b> The search is case sensitive.</p>
<b>HTTP Settings</b>	
<b>Web service server URL</b>	Shows the URL of the Web service server to be monitored.

GUI Element	Description
HTTP user agent	The HTTP user agent for the SOAP request.
HTTP content type	The content type of the HTTP request.
<b>Proxy Settings</b>	
HTTP proxy	(Optional) A proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.
Proxy server user name	If the proxy server requires a name and password to access the URL, enter the name here. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
Proxy server password	If the proxy server requires a name and password to access the URL, enter the password here. <b>Note:</b> Your proxy server must support Proxy-Authentication for these options to function.
<b>Login Settings</b>	
NTLM domain	If the Web service requires NTLM / Challenge Response authentication, a domain name is required as part of your credentials (as well as a user name and password below).

GUI Element	Description
<p><b>Authorization user name</b></p>	<p>If the web service requires a user name and password for access (Basic, Digest, or NTLM authentication), enter the user name.</p> <p>Alternately, you can leave this entry blank and enter the user name in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.</p>
<p><b>Authorization password</b></p>	<p>If the web service requires a user name and password for access (Basic, Digest or NTLM authentication), type the password.</p> <p>Alternately, you can leave this entry blank and enter the password in the Default Authentication Credentials section on the General Preferences page. You use this alternate method to define common authentication credentials for use with multiple Web Service monitor.</p>

# 98

---

## WebLogic Application Server Monitor

This chapter includes the main concepts, tasks, and reference information for the WebLogic Application Server monitor.

### **This chapter includes:**

#### **Concepts**

- ▶ WebLogic Application Server Monitor Overview on page 1062

#### **Tasks**

- ▶ Configure the WebLogic Application Server Monitoring Environment on page 1063

#### **Reference**

- ▶ WebLogic Application Server Monitor Settings on page 1066

## WebLogic Application Server Monitor Overview

Use the WebLogic Application Server monitor to monitor performance statistics data from WebLogic 6.x, 7.x, and 8.x servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning. Create a separate WebLogic Application Server monitor instance for each WebLogic server in your environment.

---

**Note:** WebLogic Application Server Monitors cannot be used to monitor WebLogic 9.x or WebLogic 10.0 - 10.2 servers. To monitor these servers, use a JMX monitor as described in “JMX Monitor Overview” on page 577. For further details, see “Creating a JMX Monitor for a WebLogic 9.x or WebLogic 10.0 - 10.2 Server” on page 580.

SiteScope can discover the topology of WebLogic application servers using the JMX monitor. You cannot use the WebLogic Application Server monitor to discover topology data for reporting to Business Availability Center. For details, see “WebLogic Application Server Topology Settings” on page 580.

If you are using a WebLogic 9.x or WebLogic 10.0 - 10.2 server, the rest of this chapter is not relevant.

---

The BEA WebLogic Application Server monitor uses the Java JMX interface to access Runtime MBeans on the WebLogic server. An MBean is a container that holds the performance data. You must set certain permissions on the WebLogic server for SiteScope to be able to monitor MBeans.

---

**Note:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a WebLogic application server. For details, see “WebLogic Solution Template” on page 1795.

---

For task details, see “Configure the WebLogic Application Server Monitoring Environment” on page 1063.

For user interface details, see “WebLogic Application Server Monitor Settings” on page 1066.

## **Configure the WebLogic Application Server Monitoring Environment**

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Set Permissions for Monitoring WebLogic 6.x Servers” on page 1063
- “Set Permissions for Monitoring WebLogic 7.x or 8.x Servers” on page 1064
- “Configure SiteScope to Use T3 Over SSL Against a WebLogic 7.x or 8.x Server” on page 1064
- “Configure the Monitor Properties” on page 1065

### **1 Set Permissions for Monitoring WebLogic 6.x Servers**

To set permissions for monitoring WebLogic 6.x servers, create a new ACL on the WebLogic server with the name **weblogic.admin.mbean**. Set the permission type to **access** and set the Users and Groups to be the user or group account that SiteScope uses to monitor the WebLogic server.

## 2 Set Permissions for Monitoring WebLogic 7.x or 8.x Servers

WebLogic 7.x and later servers use Security Policies instead of ACL's to control access to the server resources. To monitor WebLogic 7.x and later servers with SiteScope, the WebLogic administrator needs to add the user account that is running SiteScope to a WebLogic user group. The WebLogic group containing the SiteScope user must then be associated with a role statement that grants the necessary security role for accessing the desired WebLogic resources. The same security role must also be associated with the applicable policy statement that grants SiteScope access to the WebLogic resources. Refer to the WebLogic server documentation for more information.

## 3 Configure SiteScope to Use T3 Over SSL Against a WebLogic 7.x or 8.x Server

Perform the following steps to configure a WebLogic monitor with the **Secure Server** option to monitor a WebLogic 7.x or 8.x server.

- a** Obtain and install a JRE version 1.4.1 on the machine where SiteScope is running. Make a note of the full path to this JRE installation, as you must enter this information in the WebLogic monitor setup.
- b** Import the WebLogic Server's certificate, signed by a certificate authority, into the `<jre_path>\lib\security\cacerts` file for the JRE 1.4.1 installation on the SiteScope machine. If it is not, then you have to import the signer's certificate into the cacerts file using the keytool program. For instance, using the default WebLogic cert setup, you must import the **CertGenCA.der** certificate using the following command (this must all be entered on a single command line):
 

```
C:\j2sdk1.4.1\jre\bin>keytool.exe -import -alias weblogic81CA -keystore
      ..\lib\security\cacerts -trustcacerts -file
      C:\BEA\weblogic81\server\lib\CertGenCA.der
```
- c** Obtain a valid BEA license file and put it somewhere on the SiteScope machine. This is the file named **license.bea** in the BEA installation directory.
- d** Obtain the **weblogic.jar** file from the WebLogic server or from a WebLogic server of the same version that you are monitoring. For WebLogic version 8.x, you must also obtain a copy of the **wlcipher.jar** file. Copy this or these files to the SiteScope server.



---

**Note:** Do not install the **weblogic.jar** file in the SiteScope directory tree. In other words, do not install it in the **<SiteScope root directory>\java\lib\ext** directory as this causes the Weblogic monitor to fail. You must install it in a separate directory on the server where SiteScope is running.

---

- e** Open SiteScope and add a WebLogic Application Server monitor.
- f** Configure the WebLogic Application Server Monitor Settings as follows:
  - ▶ In the Authentication Settings area, select the **Secure server** option.
  - ▶ In the Advanced Settings area:
    - ▶ Enter the full path to the **wlcipher.jar** and **weblogic.jar** files in the **WLCipher jar file** and the **WebLogic jar file** boxes, respectively.
    - ▶ Enter the full path to the BEA license file in the **WebLogic license file** box.
    - ▶ Enter the full path to the **javaw.exe** (for Windows platforms) or the **java** (Solaris/Linux) executable for the JRE version 1.4.1 installation in the **JVM** box.
- g** Click the **Get Counters** button to browse the counters on the WebLogic server over SSL.

#### **4 Configure the Monitor Properties**

Complete the WebLogic Application Server monitor configuration. For details on the monitor settings, see “WebLogic Application Server Monitor Settings” on page 1066.



## WebLogic Application Server Monitor Settings

<p><b>Description</b></p>	<p>The WebLogic Application Server monitor enables you to monitor the statistics of a WebLogic version 6 through 8 servers.</p> <p>WebLogic Application Server Monitors cannot be used to monitor WebLogic 9.x or WebLogic 10.0-10.2 servers. To monitor these servers, use a JMX monitor. For further details, see “Creating a JMX Monitor for a WebLogic 9.x or WebLogic 10.0 - 10.2 Server” on page 580.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “Configure the WebLogic Application Server Monitoring Environment” on page 1063</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “WebLogic Application Server Monitor Overview” on page 1062</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## WebLogic Application Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Authentication Settings</b>	
<b>Target</b>	Enter the name of the server where WebLogic is running.
<b>Server</b>	Enter the address of the server where WebLogic is running.
<b>Port number</b>	Enter the port number that the WebLogic server is responding on. <b>Default value:</b> 7001
<b>User name</b>	Enter the user name required to log in to the WebLogic server.
<b>Password</b>	Enter the password required to log in to the WebLogic server.
<b>Secure server</b>	Select this box if you are using a secure server connection option. If you select this option, you must enter the applicable port number used by the WebLogic server for secure connections. <b>Default value:</b> 7002
<b>Advanced Settings</b>	
<b>WLCipher jar file</b>	For some versions of WebLogic Server, you must install a copy of the wlcipher.jar file from the WebLogic server onto the SiteScope server to enable monitoring over SSL. Enter the absolute path to the file on the SiteScope machine. <b>Example:</b> C:\bea\weblogic81\server\lib\wlcipher.jar <b>Note:</b> This option is for use only with the <b>Secure Server</b> (SSL) option.

GUI Element	Description
<b>WebLogic license file</b>	<p>You use this box only when you want to enable the Secure Server (SSL) option. Enter the absolute path to the BEA license file that was copied to the SiteScope machine.</p> <p><b>Example:</b> C:\bea\license.bea</p>
<b>JVM</b>	<p>Enter the full path to the Java Virtual Machine (JVM) in which the WebLogic monitoring process should be run.</p> <p>For monitors that do not use the Secure Server option, this is not required.</p> <p>For monitors which do use the Secure Server option, a separate JVM must be installed on the server where SiteScope is running. This other JVM must be version 1.4.1 or earlier. This is not the same JVM version used by SiteScope.</p> <p><b>Example:</b> C:\jdk1.4.1\bin\javaw.exe</p>
<b>WebLogic jar file</b>	<p>Enter the absolute path to the weblogic.jar file on the SiteScope machine. This file must be installed on the SiteScope server and can be downloaded from the WebLogic server.</p> <p><b>Example:</b> c:\bea\weblogic7\ebcc\lib\ext\weblogic.jar</p> <p>This file is not strictly required for monitoring some earlier versions of WebLogic 6. In this case, leaving this box blank normally causes any necessary classes to be downloaded directly from the WebLogic server. Note that this is not as efficient as loading the classes from the *.jar file on the server where SiteScope is running.</p>
<b>Classpath</b>	<p>Enter additional classpath variables that are to be used by the WebLogic JVM running on the SiteScope machine. File path elements should be separated by a colon (":") on UNIX systems, and by a semicolon (";") on Microsoft Windows systems.</p>

GUI Element	Description
<b>Timeout (seconds)</b>	<p>The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 180 (using a value other than the default timeout value may adversely affect performance)</p>
<b>Counter Settings</b>	
<b>Counters</b>	<p>The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>



# 99

---

## WebSphere Application Server Monitor

This chapter includes the main concepts, tasks, and reference information for the WebSphere Application Server monitor.

### **This chapter includes:**

#### **Concepts**

- ▶ WebSphere Application Server Monitor Overview on page 1072

#### **Tasks**

- ▶ Configure the WebSphere 3.5x and 4.x Application Server Monitoring Environment on page 1074
- ▶ Configure the WebSphere 5.x Application Server Monitoring Environment on page 1075
- ▶ Configure the WebSphere 6.0x Application Server Monitoring Environment on page 1077
- ▶ Configure the WebSphere 6.1x Application Server Monitoring Environment on page 1083
- ▶ Configure the WebSphere 7.0x Application Server Monitoring Environment on page 1090

#### **Reference**

- ▶ WebSphere Application Server Monitor Settings on page 1097

## WebSphere Application Server Monitor Overview

Use the WebSphere Application Server monitor to monitor the server performance statistics from IBM WebSphere 3.5.x, 4.x, 5.x, 6.0x, 6.1x, and 7.0x servers using the performance monitoring interfaces provided with WebSphere. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server loading for performance, availability, and capacity planning.

Create a separate WebSphere Application Server monitor instance for each WebSphere 3.5.x, 4.x, 5.x, and 7.0x Application Server in your environment. For WebSphere 6.0 and 6.1 Application Servers, you can monitor different instances of WebSphere 6.0 and 6.1 Application Servers simultaneously within one SiteScope process. Previously, you could monitor only one WebSphere 6.0 or 6.1 version at one time.

---

**Note:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of a WebSphere Application server. For details, see “WebSphere Solution Template” on page 1805.

---

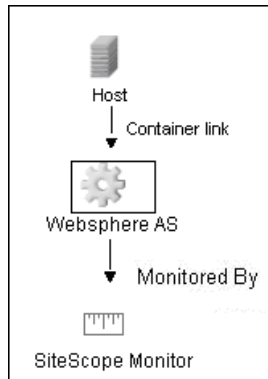
This section contains the following topics:

- “WebSphere Application Server Topology Settings” on page 1073
- “Configuring the Monitor” on page 1073



## WebSphere Application Server Topology Settings

The WebSphere Application Server monitor can identify the topology of the WebSphere Application Servers being monitored. If **Include topology data when reporting to BAC** is selected in **HP BAC Integration Settings** (the default setting), the monitor creates the following topology in Business Availability Center's CMDB.



For information about retrieving topologies and reporting them to Business Availability Center, see “Reporting Discovered Topologies to HP Business Availability Center” on page 160 in the HP Business Availability Center Documentation Library.

## Configuring the Monitor

Before you can use the WebSphere Application Server monitor, there are a number of configuration requirements involving the server environment.

For user interface details, see “WebSphere Application Server Monitor Settings” on page 1097.

## **Configure the WebSphere 3.5x and 4.x Application Server Monitoring Environment**

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Configure the WebSphere 3.5.x and 4.x Server Environment” on page 1074
- “Configure the Monitor Properties” on page 1075

### **1 Configure the WebSphere 3.5.x and 4.x Server Environment**

Perform the following to prepare the WebSphere environment for SiteScope monitoring of WebSphere versions 3.5.x and 4.x:

- a** Install the IBM WebSphere Administrator's Console on the SiteScope server if you are monitoring WebSphere versions 3.5.x or 4.x.

If installing the Administrator's Console:

- Select **Custom Installation** option during installation.
- Select **Administrator's Console** and **IBM JDK 1.2.2.** in the **Choose Application Server Components** dialog box.
- Specify the machine you want to monitor during the installation.

- b** Enable the WebSphere servers to be monitored.

- For WebSphere 3.5.x, enable EPM Counters on the WebSphere server. You can also use the WebSphere Administrator's Console to set the EPM Specification to `epm=high:epm.beanMethodData=none`.
- For WebSphere 4.x, enable PMI Counters or enable the Performance Monitoring Service on the WebSphere server. You can enable the counters for the application you want to monitor by using the WebSphere Administrator's Console.
- For WebSphere 4.x, select **Resources** and then select the **Performance** option. In the dialog box that opens, expand the **Performance Modules** tree. To manage different levels of performance data, select the performance modules, choose a performance level, and then click the **Set** button.

- c If security has been enabled on the WebSphere server, the server security ring must be copied to the admin client.

## 2 Configure the Monitor Properties

Complete the WebSphere Application Server monitor configuration. For details on the monitor settings, see “WebSphere Application Server Monitor Settings” on page 1097.

## Configure the WebSphere 5.x Application Server Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Configure the WebSphere 5.x Server Environment” on page 1075
- “Configure the Monitor Properties” on page 1077

### 1 Configure the WebSphere 5.x Server Environment

To monitor WebSphere version 5.x, the necessary WebSphere libraries must be available on the SiteScope server. Generally, this means that a WebSphere 5.x client install must exist on the SiteScope server.

- a Install the **Administration (or admin console) Performance Analysis** option from the custom options menu in the WebSphere 5.x install.

---

**Important:** Certain trial versions of IBM WebSphere do not include the Performance Analysis option required by the SiteScope WebSphere Application Server monitor. The SiteScope monitor can only work when a complete WebSphere production installation is available.

---

- b Copy all of the files from the **lib** folder of a WebSphere 5.x Application Server installation to the **lib** folder on the client install from step 1.

- c** The WebSphere 5.x server and client settings have to match. This means that the SiteScope WebSphere Application Server monitor is not able to monitor a WebSphere 5.1 application server if the client libraries are from a WebSphere 5.0 and vice versa. Client libraries should be installed in separate folders with clearly distinct directory names (for example, Websphere50 and Websphere51) to avoid confusion and SiteScope setup errors.

---

**Note:** For WebSphere 5.x SiteScope uses the WebSphere JMX interface so the port number used to communicate with the application server is the SOAP port number. The default SOAP port number is 8880.

---

- d** Enable PMI Counters or the Performance Monitoring Service on the WebSphere server. You can enable the counters for the application you want to monitor by using the WebSphere Administrator's Console.
  - Click **Servers > Application Servers**.
  - Select the server to be monitored from the Application Server list.
  - From the Configuration tab, click the Performance Monitoring Service in the Additional Properties list.
  - Select the **Start Up** check box and select the **Initial specification** level as Standard or Custom.
  - Click **Apply**.
- e** If security has been enabled on the WebSphere server, the server security ring must be copied to the admin client.

---

**Note:** If security has been enabled on the WebSphere 5.x server, you must copy the security keyring from the WebSphere server to SiteScope. A keyring is a certification used by the server to identify the client.

---

## 2 Configure the Monitor Properties

Complete the WebSphere Application Server monitor configuration. For details on the monitor settings, see “WebSphere Application Server Monitor Settings” on page 1097.

## Configure the WebSphere 6.0x Application Server Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Configure the WebSphere 6.0x Server Environment” on page 1077
- “Configure the Monitor Properties” on page 1078
- “Monitor Different Instances Simultaneously” on page 1078

### 1 Configure the WebSphere 6.0x Server Environment

Configure the WebSphere version 6.0x monitoring environment according to whether you are using internal or external Java.

- For details on configuring the WebSphere 6.0x monitoring environment using internal Java, see “Configure the WebSphere 6.0x Server Environment Using Internal Java” on page 1079.
- For details on configuring the WebSphere 6.0x monitoring environment using external Java, see “Configure the WebSphere 6.0x Server Environment Using External Java” on page 1080.

## 2 Configure the Monitor Properties

Create the WebSphere Application Server monitor, and enter the following information in the Monitor Settings panel:

- **WebSphere directory:** %WAS\_ENV%
  - **Trust store:** %WAS\_ENV%\DummyClientTrustFile.jks
  - **Trust store password:** WebAS
  - **Key store:** %WAS\_ENV%\DummyClientKeyFile.jks
  - **Key store password:** WebAS
- 

### Note:

- If you configured the WebSphere environment to use internal JVMs, make sure that the **Launch an external JVM** check box is not selected. By default, the WebSphere monitor uses internal JVMs for new monitors. When upgrading from previous versions of SiteScope, this check box is selected automatically during the upgrade for existing monitors.
  - You can use certificates added using Certificate Management only if **Launch an external JVM** is not selected.
  - When using SSL, you also need to define the **User name** and **Password** to access the WebSphere Application Server.
- 

For details on the monitor settings, see “WebSphere Application Server Monitor Settings” on page 1097.

## 3 Monitor Different Instances Simultaneously

After configuring settings for the WebSphere Application Server monitor version 6.0x, select **6.1x** from the **Version** drop-down list. The monitor runs simultaneously with the monitor that you just created for WebSphere version 6.0x.

**Note:** To monitor a WebSphere version 6.1x simultaneously, you must have configured the WebSphere version 6.1x monitoring environment. For details, see “Configure the WebSphere 6.1x Application Server Monitoring Environment” on page 1083.

## **Configure the WebSphere 6.0x Server Environment Using Internal Java**

To enable monitoring WebSphere version 6.0x, you must configure the server environment.

**To configure the WebSphere 6.0x server environment using internal Java:**

- 1** On the SiteScope machine, create a directory and give it a name, for example, C:\WAS\_6. This directory is referred to as %WAS\_ENV%, and the SiteScope root folder is referred to as %SIS\_HOME% (you should replace all appearances of %WAS\_ENV% and %SIS\_HOME% with the actual value).
- 2** Copy the following contents from WebSphere Application Server to the SiteScope machine:

From WebSphere Application Server:	To SiteScope machine:
Copy the entire folder: <WAS_SERVER>\WebSphere\AppServer\lib	%WAS_ENV%\lib
<WAS_SERVER>\WebSphere\AppServer\java\jre\lib\ibmcertpathprovider.jar	%WAS_ENV%\ibmcertpathprovider.jar
<WAS_SERVER>\WebSphere\AppServer\java\jre\lib\ext\ibmjceprovider.jar	%WAS_ENV%\ibmjceprovider.jar
<WAS_SERVER>\WebSphere\AppServer\profiles\<ServerName>\etc\DummyClientTrustFile.jks	%WAS_ENV%\
<WAS_SERVER>\WebSphere\AppServer\profiles\<ServerName>\etc\DummyClientKeyFile.jks	%WAS_ENV%\

- 3 (SSL only) Import the SSL server certificates. You can use Certificate Management to import the certificates, or you can import the certificates manually.
  - For details on importing certificates using Certificate Management, see “Import Server Certificates Using Certificate Management” on page 1537.
  - For details on importing certificates manually, see “Import Server Certificates Manually for WebSphere 6.0x” on page 1082.
- 4 After importing the server certificates, restart the SiteScope server.
- 5 Continue with step 2 on page 1078.

### **Configure the WebSphere 6.0x Server Environment Using External Java**

To enable monitoring WebSphere version 6.0x, you must configure the server environment.

**To configure the WebSphere 6.0x server environment using external Java:**

- 1 You must have the following directories copied onto the SiteScope machine:
  - AppServer/Java
  - AppServer/lib

These directories must be copied into any directory on the SiteScope machine but must be stored exactly as they appear under the **AppServer** directory.

You can use one of the following options:

- Create a directory on the machine running SiteScope called **AppServer** and copy the two directories, **Java** and **lib**, directly into the newly created **AppServer** directory. We recommend option because it occupies the least amount of disk space on your SiteScope machine.
- Copy the entire WebSphere AppServer directory from the machine being monitored onto the machine running SiteScope.



- Copy all the WebSphere application server files onto the machine running SiteScope. We do not recommend this option because of the size of the application server files.

Once you have the **AppServer/Java** and **Appserver/lib** files on the SiteScope machine, use the following procedure to prepare the WebSphere environment for monitoring WebSphere 6.x.

- 2** On the WebSphere server, select **Servers > Application Servers > <server name> > Performance Monitoring Infrastructure (PMI)** and make sure that the counters are set to **Extended**.
- 3** From the SiteScope machine, make sure that you can access the SOAP from a browser. For example, open a browser and enter the following sample address: `http://jberantlab:8880`. If an XML page is returned, the monitor is ready to be added to SiteScope and configured.

---

**Note:** For WebSphere 6.x and later, SiteScope uses the WebSphere JMX interface so the port number used to communicate with the application server is the SOAP port number. The default SOAP port number is 8880.

---

- 4** Continue with step 2 on page 1078.

## **Import Server Certificates Manually for WebSphere 6.0x**

Instead of using Certificate Management, you can import certificates manually using the keytool method, if preferred. Certificates imported this way can still be managed using Certificate Management. For details on Certificate Management, see “Certificate Management” on page 1535.

### To import server certificates manually:

- 1** Using Internet Explorer 6 or 7, export the SSL certificate to `%WAS_ENV%\was_certificate.cert` (in base-64 format).
  - a** Download the server certificate by double-clicking the key lock icon in Internet Explorer when there is an SSL connection. The icon is located in the status bar for Internet Explorer 6, and to the right of the URL field for Internet Explorer 7 (the field is marked red when self-signed certified is used by the server).
  - b** In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
  - c** In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- 2** Import the certificate to the `cacerts` file in the SiteScope java folder as follows:

```
%SIS_HOME%\java\bin\keytool -import -v -file %WAS_ENV%\was_certificate.cert -alias was_cert -keystore %SIS_HOME%\java\lib\security\cacerts
```

When prompted for the password, type `changeit` (default password for JRE).

When asked if you trust the imported certificate, type `yes`.

- 3** Continue with step 4 on page 1080.

## **Configure the WebSphere 6.1x Application Server Monitoring Environment**

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Configure the WebSphere 6.1x Server Environment Using Internal Java” on page 1085
- “Configure the Monitor Properties” on page 1083
- “Monitor Different Instances Simultaneously” on page 1084

### **1 Configure the WebSphere 6.1x Server Environment**

Configure the WebSphere version 6.1x monitoring environment according to whether you are using internal or external Java.

- For details on configuring the WebSphere 6.1x monitoring environment using internal Java, see “Configure the WebSphere 6.1x Server Environment Using Internal Java” on page 1085.
- For details on configuring the WebSphere 6.1x monitoring environment using external Java, see “Configure the WebSphere 6.1x Server Environment Using External Java” on page 1087.

### **2 Configure the Monitor Properties**

Create the WebSphere Application Server monitor, and enter the following information in the Monitor Settings panel:

- **WebSphere directory:** %WAS\_ENV%
- **Trust store:** %WAS\_ENV%\DummyClientTrustFile.jks
- **Trust store password:** WebAS
- **Key store:** %WAS\_ENV%\DummyClientKeyFile.jks
- **Key store password:** WebAS

**Note:**

- ▶ If you configured the WebSphere environment to use internal JVMs, make sure that the **Launch an external JVM** check box is not selected. By default, the WebSphere monitor uses internal JVMs for new monitors. When upgrading from previous versions of SiteScope, this check box is selected automatically during the upgrade for existing monitors.
  - ▶ You can use certificates added using Certificate Management only if **Launch an external JVM** is not selected.
  - ▶ When using SSL, you also need to define the **User name** and **Password** to access the WebSphere Application Server.
- 

For details on the monitor settings, see “WebSphere Application Server Monitor Settings” on page 1097.

### **3 Monitor Different Instances Simultaneously**

To monitor a WebSphere version 6.0x simultaneously, choose **6.0x** from the **Version** drop-down list. The monitor runs simultaneously with the monitor that you just created for WebSphere version 6.1x.

## Configure the WebSphere 6.1x Server Environment Using Internal Java

To enable monitoring WebSphere version 6.1x, you must configure the server environment.

**To enable monitoring WebSphere version 6.1x using internal Java:**

- 1 On the SiteScope machine, create a directory and give it a name, for example, C:\WAS\_6\_1. This directory is referred to as %WAS\_ENV%, and the SiteScope root folder is referred to as %SIS\_HOME% (you should replace all appearances of %WAS\_ENV% and %SIS\_HOME% with the actual value).
- 2 Copy the following contents from WebSphere Application Server to the SiteScope machine:

From WebSphere Application Server:	To SiteScope machine:
<WAS_SERVER>\WebSphere\ AppServer\plugins\ com.ibm.ws.security.crypto_6.1.0.jar	%SIS_HOME% \java\lib\ext\ com.ibm.ws.security.crypto_6.1.0.jar
<WAS_SERVER>\WebSphere\ AppServer\runtimes\ com.ibm.ws.admin.client_6.1.0.jar	%WAS_ENV%\ com.ibm.ws.admin.client_6.1.0.jar
<WAS_SERVER>\plugins\ com.ibm.ws.runtime_6.1.0.jar	%WAS_ENV%\ com.ibm.ws.runtime_6.1.0.jar
<WAS_SERVER>\WebSphere\ AppServer\profiles\<<ServerName>\ etc\DummyClientTrustFile.jks	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\profiles\<<ServerName>\ etc\DummyClientKeyFile.jks	%WAS_ENV%\

- 3** (SSL only) Import the SSL server certificates. You can use Certificate Management to import the certificates, or you can import the certificates manually.
  - For details on importing certificates using Certificate Management, see “Import Server Certificates Using Certificate Management” on page 1537.
  - For details on importing certificates manually, see “Import Server Certificates Manually for WebSphere 6.1x” on page 1089.
- 4** After importing the server certificates, modify the `%SIS_HOME%\java\lib\security\java.security` file so that it reads as follows:

```
# Default JSSE socket factories
ssl.SocketFactory.provider=com.sun.net.ssl.internal.ssl.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.sun.net.ssl.internal.ssl.SSLServerSocketFactoryImpl
```

- 5** Restart the SiteScope server.
- 6** Continue with step 2 on page 1083.

## Configure the WebSphere 6.1x Server Environment Using External Java

To enable monitoring WebSphere version 6.1x, you must configure the server environment.

**To configure the WebSphere 6.1x server environment using external Java:**

- 1** On the SiteScope machine, create a directory and give it a name, for example, C:\WAS\_6\_1. This directory is referred to as %WAS\_ENV% (you should replace all appearances of %WAS\_ENV% with the actual value).
- 2** Copy the following contents from WebSphere Application Server to the SiteScope machine:

From WebSphere Application Server:	To SiteScope machine:
<WAS_SERVER>\java\**\*.*	%WAS_ENV%\java\**\*.*
<WAS_SERVER>\runtimes\ com.ibm.ws.admin.client_6.1.0.jar	%WAS_ENV%\com.ibm.ws.admin. client_6.1.0.jar
<WAS_SERVER>\plugins\ com.ibm.ws.runtime_6.1.0.jar	%WAS_ENV%\com.ibm.ws. runtime_6.1.0.jar
<WAS_SERVER>\WebSphere\ AppServer\profiles\<<ServerName>\ etc\DummyClientTrustFile.jks	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\profiles\<<ServerName>\ etc\DummyClientKeyFile.jks	%WAS_ENV%\

- 3** (SSL only) Using Internet Explorer 6 or 7, export the SSL certificate to %WAS\_ENV%\was\_certificate.cert (in base-64 format).
  - a** Download the server certificate by double-clicking the key lock icon in Internet Explorer when there is an SSL connection. The icon is located in the status bar for Internet Explorer 6, and to the right of the URL field for Internet Explorer 7 (the field is marked red when self-signed certified is used by the server).
  - b** In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.

- c** In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- 4** (SSL only) Import the certificate to the **cacerts** file in the above java folder as follows:

```
%WAS_ENV%\java\bin\keytool -import -v -file %WAS_ENV%\was_certificate.cert -alias was_cert -keystore %WAS_ENV%\java\jre\lib\security\cacerts
```

When prompted for the password, type **changeit** (default password for JRE).

When asked if you trust the imported certificate, type **yes**.

- 5** Modify the **%WAS\_ENV%\java\jre\lib\security\java.security** file so that it reads as follows:

```
== FROM ==
# Default JSSE socket factories
#ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
#ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
# WebSphere socket factories (in cryptosf.jar)
ssl.SocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory
ssl.ServerSocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLServerSocketFactory

== TO ==
# Default JSSE socket factories
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
# WebSphere socket factories (in cryptosf.jar)
#ssl.SocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory
#ssl.ServerSocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLServerSocketFactory
```

- 6** Restart the SiteScope machine.
- 7** Continue with step 2 on page 1083.



## Import Server Certificates Manually for WebSphere 6.1x

Instead of using Certificate Management, you can import certificates manually using the keytool method, if preferred. Certificates imported this way can still be managed using Certificate Management. For details on Certificate Management, see “Certificate Management” on page 1535.

### To import server certificates manually:

- 1** Using Internet Explorer 6 or 7, export the SSL certificate to `%WAS_ENV%\was_certificate.cert` (in base-64 format).
  - a** Download the server certificate by double-clicking the key lock icon in Internet Explorer when there is an SSL connection. The icon is located in the status bar for Internet Explorer 6, and to the right of the URL field for Internet Explorer 7 (the field is marked red when self-signed certified is used by the server).
  - b** In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
  - c** In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- 2** Import the certificate to the `cacerts` file in the SiteScope java folder as follows:
 

```
%SIS_HOME%\java\bin\keytool -import -v -file %WAS_ENV%\was_certificate.cert -alias was_cert -keystore %SIS_HOME%\java\lib\security\cacerts
```

When prompted for the password, type `changeit` (default password for JRE).  
When asked if you trust the imported certificate, type `yes`.
- 3** Continue with step 4 on page 1086.

## **Configure the WebSphere 7.0x Application Server Monitoring Environment**

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Configure the WebSphere 7.0x Server Environment” on page 1090
- “Configure the Monitor Properties” on page 1090

### **1 Configure the WebSphere 7.0x Server Environment**

Configure the WebSphere version 7.0x monitoring environment according to whether you are using internal or external Java.

- For details on configuring the WebSphere 7.0x monitoring environment using internal Java, see “Configure the WebSphere 7.0x Server Environment Using Internal Java” on page 1092.
- For details on configuring the WebSphere 7.0x monitoring environment using external Java, see “Configure the WebSphere 7.0x Server Environment Using External Java” on page 1094.

### **2 Configure the Monitor Properties**

Create the WebSphere Application Server monitor, and enter the following information in the Monitor Settings panel:

- **WebSphere directory:** %WAS\_ENV%
- **Trust store:** %WAS\_ENV%\DummyClientTrustFile.jks
- **Trust store password:** WebAS
- **Key store:** %WAS\_ENV%\DummyClientKeyFile.jks
- **Key store password:** WebAS

**Note:**

- ▶ If you configured the WebSphere environment to use internal JVMs, make sure that the **Launch an external JVM** check box is not selected. By default, the WebSphere monitor uses internal JVMs for new monitors. When upgrading from previous versions of SiteScope, this check box is selected automatically during the upgrade for existing monitors.
  - ▶ You can use certificates added using Certificate Management only if **Launch an external JVM** is not selected.
  - ▶ When using SSL, you also need to define the **User name** and **Password** to access the WebSphere Application Server.
- 

For details on the monitor settings, see “WebSphere Application Server Monitor Settings” on page 1097.

## Configure the WebSphere 7.0x Server Environment Using Internal Java

To enable monitoring WebSphere version 7.0x, you must configure the server environment.

**To enable monitoring WebSphere version 7.0x using internal Java:**

- 1** On the SiteScope machine, create a directory and give it a name, for example, C:\WAS\_7. This directory is referred to as %WAS\_ENV%, and the SiteScope root folder is referred to as %SIS\_HOME% (you should replace all appearances of %WAS\_ENV% and %SIS\_HOME% with the actual value).
- 2** Copy the following contents from WebSphere Application Server to the SiteScope machine:

From WebSphere Application Server:	To SiteScope machine:
<WAS_SERVER>\WebSphere\ AppServer\plugins\ com.ibm.ws.security.crypto.jar	%SIS_HOME% \java\lib\ext\ com.ibm.ws.security.crypto.jar
<WAS_SERVER>\WebSphere\ AppServer\runtimes\ com.ibm.ws.admin.client.jar	%WAS_ENV%\ com.ibm.ws.admin.client.jar
<WAS_SERVER>\WebSphere\ AppServer\plugins\ com.ibm.ws.runtime.jar	%WAS_ENV%\ com.ibm.ws.runtime.jar
<WAS_SERVER>\WebSphere\ AppServer\profiles\<<ServerName>\ etc\DummyClientTrustFile.jks	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\profiles\<<ServerName>\ etc\DummyClientKeyFile.jks	%WAS_ENV%\

- 3** (SSL only) Import the SSL server certificates. You can use Certificate Management to import the certificates, or you can import the certificates manually.
  - For details on importing certificates using Certificate Management, see “Import Server Certificates Using Certificate Management” on page 1537.
  - For details on importing certificates manually, see “Import Server Certificates Manually for WebSphere 7.0x” on page 1096.
- 4** After importing the server certificates, modify the `%SIS_HOME%\java\lib\security\java.security` file so that it reads as follows:

```
# Default JSSE socket factories
ssl.SocketFactory.provider=com.sun.net.ssl.internal.ssl.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.sun.net.ssl.internal.ssl.SSLServerSocketFactoryImpl
```

- 5** Restart the SiteScope server.
- 6** Continue with step 2 on page 1090.

## Configure the WebSphere 7.0x Server Environment Using External Java

To enable monitoring WebSphere version 7.0x, you must configure the server environment.

**To configure the WebSphere 7.0x server environment using external Java:**

- 1** On the SiteScope machine, create a directory and give it a name, for example, C:\WAS\_7. This directory is referred to as %WAS\_ENV% (you should replace all appearances of %WAS\_ENV% with the actual value).
- 2** Copy the following contents from WebSphere Application Server to the SiteScope machine:

From WebSphere Application Server:	To SiteScope machine:
<WAS_SERVER>\java\**\*.*	%WAS_ENV%\java\**\*.*
<WAS_SERVER>\runtimes\com.ibm.ws.admin.client_7.0.0.jar	%WAS_ENV%\com.ibm.ws.admin.client_7.0.0.jar
<WAS_SERVER>\plugins\com.ibm.w s.runtime.jar	%WAS_ENV%\com.ibm.ws.runtime.jar
<WAS_SERVER>\WebSphere\AppServer\profiles\<ServerName>\etc\DummyClientTrustFile.jks	%WAS_ENV%\
<WAS_SERVER>\WebSphere\AppServer\profiles\<ServerName>\etc\DummyClientKeyFile.jks	%WAS_ENV%\

- 3** (SSL only) Using Internet Explorer 6 or 7, export the SSL certificate to %WAS\_ENV%\was\_certificate.cert (in base-64 format).
  - a** Download the server certificate by double-clicking the key lock icon in Internet Explorer when there is an SSL connection. The icon is located in the status bar for Internet Explorer 6, and to the right of the URL field for Internet Explorer 7 (the field is marked red when self-signed certified is used by the server).
  - b** In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.

- c** In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- 4** (SSL only) Import the certificate to the **cacerts** file in the above java folder as follows:

```
%WAS_ENV%\java\bin\keytool -import -v -file %WAS_ENV%\was_certificate.cert -alias was_cert -keystore %WAS_ENV%\java\jre\lib\security\cacerts
```

When prompted for the password, type **changeit** (default password for JRE).

When asked if you trust the imported certificate, type **yes**.

- 5** Modify the **%WAS\_ENV%\java\jre\lib\security\java.security** file so that it reads as follows:

```
== FROM==
# Default JSSE socket factories
#ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
#ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
# WebSphere socket factories (in cryptosf.jar)
ssl.SocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory
ssl.ServerSocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLServerSocketFactory

==TO==
# Default JSSE socket factories
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
# WebSphere socket factories (in cryptosf.jar)
#ssl.SocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory
#ssl.ServerSocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLServerSocketFactory
```

- 6** Restart the SiteScope machine.
- 7** Continue with step 2 on page 1090.

## **Import Server Certificates Manually for WebSphere 7.0x**

Instead of using Certificate Management, you can import certificates manually using the keytool method, if preferred. Certificates imported this way can still be managed using Certificate Management. For details on Certificate Management, see “Certificate Management” on page 1535.

### To import server certificates manually:

- 1** Using Internet Explorer 6 or 7, export the SSL certificate to `%WAS_ENV%\was_certificate.cert` (in base-64 format).
  - a** Download the server certificate by double-clicking the key lock icon in Internet Explorer when there is an SSL connection. The icon is located in the status bar for Internet Explorer 6, and to the right of the URL field for Internet Explorer 7 (the field is marked red when self-signed certified is used by the server).
  - b** In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
  - c** In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- 2** Import the certificate to the `cacerts` file in the SiteScope java folder as follows:

```
%SIS_HOME%\java\bin\keytool -import -v -file %WAS_ENV%\was_certificate.cert -alias was_cert -keystore %SIS_HOME%\java\lib\security\cacerts
```

When prompted for the password, type `changeit` (default password for JRE).  
When asked if you trust the imported certificate, type `yes`.
- 3** Continue with step 4 on page 1093.





## WebSphere Application Server Monitor Settings

<b>Description</b>	<p>The WebSphere Application Server monitor enables you to monitor the availability and server statistics of an IBM WebSphere Application Server 3.5.x, 4.x, 5.x, 6.0x, 6.1x, and 7.0x. The error and warning thresholds for the monitor can be set on one or more WebSphere Application Server performance statistics.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the WebSphere 3.5x and 4.x Application Server Monitoring Environment” on page 1074</li> <li>▶ “Configure the WebSphere 5.x Application Server Monitoring Environment” on page 1075</li> <li>▶ “Configure the WebSphere 6.0x Application Server Monitoring Environment” on page 1077</li> <li>▶ “Configure the WebSphere 6.1x Application Server Monitoring Environment” on page 1083</li> <li>▶ “Configure the WebSphere 7.0x Application Server Monitoring Environment” on page 1090</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “WebSphere Application Server Monitor Overview” on page 1072</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## WebSphere Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Target</b>	Enter the logical name of the server you want to monitor. If this box is left empty, the host name entered above is used.
<b>Server</b>	Enter the name of the server where the WebSphere Application Server you want to monitor is running. <b>Note:</b> Do not include backslashes in the name.
<b>Launch an external JVM</b>	Select this option to use external JVMs. By default, the WebSphere monitor uses internal JVMs. External JVMs consume greater resources, take longer to start up, and have bad error handling. <b>Note:</b> You cannot use certificates added using Certificate Management if this setting is selected. <b>Default value:</b> Not selected (if upgrading from previous versions of SiteScope, this check box is selected automatically during the upgrade for existing monitors).
<b>Port number</b>	Enter the port number for the SOAP. <b>Default value:</b> 8880

GUI Element	Description
<b>Credentials</b>	<p>The user name and password required to access the WebSphere Application Server. Select the option to use for providing credentials:</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials. Enter the user name and password in the <b>User name</b> and <b>Password</b> box if one has been configured.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password (selected by default). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>Security realm</b>	Only relevant for WebSphere 3.5 users. Specify the security realm of the WebSphere application server.
<b>Version</b>	<p>Enter the version of the WebSphere application you are monitoring (3.5x, 4.x, 5.x, 6.0x, 6.1x, 7.0x).</p> <p><b>Default value:</b> 3.5x</p>
<b>WebSphere directory</b>	<ul style="list-style-type: none"> <li>▶ For 3.x: Enter the path to a WebSphere 3.5x Directory. The directory you enter here should contain at least a valid Admin Client installation.</li> <li>▶ For 6.x: Enter the path to the AppServer directory.</li> </ul> <p><b>Default value:</b> C:\WebSphere\AppServer</p>
<b>Client properties file</b>	<p>The name of the custom client properties file.</p> <p><b>Default value:</b> soap.client.props (use the default for version 6.x)</p>
<b>Classpath</b>	Enter additional classpath variables that are to be used by the WebSphere JVM running on the SiteScope machine.

GUI Element	Description
<p><b>Timeout (seconds)</b></p>	<p>Enter the time, in seconds, that the monitor should wait for a response from the server. If a response is not received within the interval of the timeout, the monitor reports a timeout error.</p> <p><b>Default value:</b> 60 seconds</p>
<p><b>Trust store</b></p>	<p>This is the full directory path of file <b>DummyClientTrustFile.jks</b>. The trust file is typically used to store signer certificates, which specify whether the signer of the server's certificate is trusted. This file is in the client monitor directory on the SiteScope machine.</p> <p><b>Default value:</b> C:\WebSphere\AppServer\profiles\default\etc\DummyClientTrustFile.jks</p>
<p><b>Trust store password</b></p>	<p>This is the password for the SSL trust store file.</p> <p><b>Default value:</b> WebAS</p>
<p><b>Key store</b></p>	<p>This is the full directory path of file <b>DummyClientKeyFile.jks</b>. This file is typically used to store personal certificates, including private keys. This file is in the client monitor directory on the SiteScope machine.</p> <p><b>Default value:</b> C:\WebSphere\AppServer\profiles\default\etc\DummyClientTrustFile.jks</p>

GUI Element	Description
<b>Key store password</b>	<p>This is the password for the SSL key store file.</p> <p><b>Default value:</b> WebAS</p> <p>The values for <b>Trust Store</b>, <b>Trust Store Password</b>, <b>Key Store</b>, and <b>Key Store Password</b> are automatically configured and can be found in the following directories:</p> <ul style="list-style-type: none"> <li>▶ On Windows platform, in &lt;drive&gt;:\WebSphere\AppServer\etc\</li> <li>▶ On Solaris platform, in /opt/WebSphere/AppServer/etc/</li> <li>▶ On Linux platform, in /opt/IBMWebAS/etc/</li> </ul> <p>For more information about Key Store passwords, refer to the IBM Information Center (<a href="http://publib.boulder.ibm.com/infocenter/wasinfo/v4r0/index.jsp?topic=/com.ibm.websphere.v4.doc/wasa_content/050703.html">http://publib.boulder.ibm.com/infocenter/wasinfo/v4r0/index.jsp?topic=/com.ibm.websphere.v4.doc/wasa_content/050703.html</a>) and search for SSL configuration.</p>
<b>Counters</b>	<p>The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p>
<b>Get Counters</b>	<p>Click to open the Get Counters dialog box, and select the counters you want to monitor.</p> <p><b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</p>



# 100

---

## WebSphere MQ Status Monitor

This chapter includes the main concepts, tasks, and reference information for the WebSphere MQ Status monitor.

### **This chapter includes:**

#### **Concepts**

- ▶ WebSphere MQ Status Monitor Overview on page 1104

#### **Tasks**

- ▶ Configure the WebSphere MQ Status Monitoring Environment on page 1107

#### **Reference**

- ▶ Channel Status Codes on page 1109
- ▶ WebSphere MQ Status Monitor Settings on page 1110

## WebSphere MQ Status Monitor Overview

Use the WebSphere MQ Status monitor to monitor the performance attributes of MQ Objects: channels and queues, on MQ (formerly known as MQSeries) Servers 5.2, 5.3, 5.3.1, 6.0, and 7.0. You can monitor both performance attributes and events for channels and queues.

---

**Note:** The WebSphere MQ Status monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

---

You can set the error and warning thresholds for the WebSphere MQ Status monitor on as many as fifteen function measurements.

This section contains the following topics:

- “Setup Requirements” on page 1104
- “Monitoring MQ Events” on page 1105
- “Authentication” on page 1106
- “Configuring the Monitor” on page 1106

### **Setup Requirements**

This monitor requires two IBM MQ SupportPacs to be downloaded from the IBM Web site and installed on the machine where the SiteScope server is running. For details on how to perform this task, see “Configure the WebSphere MQ Status Monitoring Environment” on page 1107.



## Monitoring MQ Events

For events, two system queues are regularly polled for the presence of relevant events:

- SYSTEM.ADMIN.PERFM.EVENT - for queue performance events
- SYSTEM.ADMIN.CHANNEL.EVENT - for channel events

On each scheduled run of the MQ monitor (which contain event counters), one or both of these system queues are queried for the presence of events that match the chosen event type, the source queue or channel that generated the event, and its queue manager. Events found are only browsed and not removed from the queue, so such events can continue to be consumed by other applications, if necessary. On each run the MQ monitor reports the number of event occurrences found since the last run of the monitor.

The monitor strives not to report the same event occurrence more than once. This is accomplished by recording the timestamp of the most recent event browsed, so that in the next monitor run any events encountered that were generated prior to this recorded timestamp are ignored.

### Enabling Queue Events on the MQ Server

By default, queue performance events are unavailable in the MQ server. For SiteScope to monitor these events, enable the MQ server to create these events. A MQSC command must be issued on each queue and for each event to be enabled. In addition, required threshold values must be set on each queue and for each event that specify the conditions for generating the event. Consult the IBM MQ MQSC Command Reference for more information. Channel events are always enabled and require no further action for them to operate.

### Specifying Alternate Queue Managers

It is possible to set up an MQSeries environment such that events from remote queue managers are routed to a central queue manager for monitoring. If the event configured for monitoring by the user is from a remote queue manager (a queue manager other than the one identified in **Queue manager** of the MQ Status Monitor Settings panel), it must be specified in the **Alternate queue manager** text box.

## Authentication

Your MQ server may require SiteScope to authenticate itself when connecting to retrieve metrics. A function has been built into this monitor to run a user-developed, client-side security exit written in Java.

To use this function, specify the fully-qualified class name of the security exit component in file `<SiteScope root directory>\groups\master.config`. For example,

```
_mqMonitorSecurityExit=com.mycompany.mq.MyExit
```

where the security exit class is called `com.mycompany.mq.MyExit`.

Make sure this class is in the classpath of the running SiteScope JVM by copying your security exit class into `<SiteScope root directory>\java\lib\ext`. You can only deploy one security exit class for a SiteScope instance, and every MQ monitor running on that instance runs that security exit.

In the case of a Windows-based SiteScope instance monitoring a Windows-based MQ server, the default authentication scheme requires that SiteScope be running under a user account that is recognized by the target server's Windows security group. Specifically, the SiteScope user must be added to the server's `mqm` group.

For information about MQ security exits and other authentication schemes, consult the IBM WebSphere MQ documentation.

## Configuring the Monitor

For task details, see “Configure the WebSphere MQ Status Monitoring Environment” on page 1107.

For user interface details, see “WebSphere MQ Status Monitor Settings” on page 1110.

## Configure the WebSphere MQ Status Monitoring Environment

This task describes the steps involved in configuring the monitoring environment.

This task includes the following steps:

- “Download and Install the IBM MQ SupportPacs” on page 1107
- “Deploy a Security Exit Class (if MQ Server Requires SiteScope Authentication)” on page 1108
- “Configure the Monitor Properties” on page 1108

### 1 Download and Install the IBM MQ SupportPacs

- a** Download the following IBM MQ SupportPacs from the IBM Web site and install them on the machine where the SiteScope server is running:
  - **MA88.** MQSeries classes for Java, version 5.2.2 (5648-C60) or later. Go to the IBM Web site for this support package. In some cases, this component may already be bundled with the IBM MQ Server installation. Check your IBM MQ install documentation for details.
  - **MS0B.** WebSphere MQ Java classes for PCF. Go to the IBM Web site for this support package.

Follow the instructions for installing both support packs.

- b** Copy the following files from these installations to the `<SiteScope root directory>\java\lib\ext` directory:
  - **com.ibm.mq.jar**
  - **connector.jar**
  - For PCF: **com.ibm.mq.pcf.jar** (for WebSphere MQ versions earlier than 6.x); **pcf.jar** (for WebSphere MQ 6.x and later)
- c** After installing the required libraries, stop and restart SiteScope.

## 2 Deploy a Security Exit Class (if MQ Server Requires SiteScope Authentication)

If the MQ server requires SiteScope to authenticate itself when connecting to retrieve metrics, specify the fully-qualified class name of the security exit component in file `<SiteScope root directory>\groups\master.config`. For example,

```
_mqMonitorSecurityExit=com.mycompany.mq.MyExit
```

where the security exit class is called `com.mycompany.mq.MyExit`.

Make sure this class is in the classpath of the running SiteScope JVM by copying your security exit class into `<SiteScope root directory>\java\lib\ext`. You can deploy only one security exit class for a SiteScope instance, and every MQ monitor running on that instance runs that security exit.

---

**Note:** For a Windows-based SiteScope instance monitoring a Windows-based MQ server, the default authentication scheme requires that SiteScope be running under a user account that is recognized by the target server's Windows security group. Specifically, the SiteScope user must be added to the server's `mqm` group.

---

For information about MQ security exits and other authentication schemes, consult the IBM WebSphere MQ documentation.

## 3 Configure the Monitor Properties

Complete the WebSphere MQ Status monitor configuration. For details on the monitor settings, see “WebSphere MQ Status Monitor Settings” on page 1110.

## Channel Status Codes

You can choose from two different reporting schemes for Channel status code values:

- ▶ **IBM MQ coding scheme.** Report the actual or original channel status codes as documented in the IBM MQ literature.
- ▶ **HP coding scheme.** Report channel status codes in ascending values that are directly proportional to the health of the channel. That is, SiteScope reports a channel status value from 0 (least healthy) to 6 (healthiest). This scheme is consistent with how other HP products report MQ channel status codes. However this scheme provides less gradients than the IBM scheme, as shown in the table below:

MQ Channel Status	MQ Coding Scheme	HP Coding Scheme
Stopped	6	0
Paused	8	0
Inactive	-1	0
Initializing	4	1
Stopping	13	1
Starting	2	2
Retrying	5	3
Requesting	7	4
Binding	1	5
Running	3	6
Stopped	6	0

You can select the required coding scheme in the **Channel status code scheme** box under WebSphere MQ Status Monitor Settings.



 **WebSphere MQ Status Monitor Settings**

<b>Description</b>	<p>The WebSphere MQ Status monitor enables you to monitor the performance attributes of MQ Objects (channels and queues) on MQ Servers. Both performance attributes and events for channels and queues can be monitored.</p> <p>This monitor was formerly known as MQSeries.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This monitor is an optional SiteScope function. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information.</li> <li>▶ Monitors must be created in a group in the monitor tree.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure the WebSphere MQ Status Monitoring Environment” on page 1107</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “WebSphere MQ Status Monitor Overview” on page 1104</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## WebSphere MQ Status Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>MQ server name</b>	Specify the host name of the MQ Server you want to monitor. Enter the network name of the server or the IP address of the server. <b>Example:</b> mqmachinename
<b>MQ server port</b>	Specify the port number of the target MQ Server. <b>Default value:</b> 1414
<b>Server connection channel</b>	Enter the name of the server connection channel of the target MQ server. Check with the MQ Server administrator for the name syntax of the server connection channel.
<b>Queue manager</b>	Enter the name of the queue manager whose queues or channels are to be monitored.
<b>User name</b>	Enter the user name for the MQ Server you want to monitor. To connect to the server using the SiteScope user, leave this field and the <b>Password</b> empty.
<b>Password</b>	Enter the password for the MQ Server you want to monitor. To connect to the server using the SiteScope user, leave this field and the <b>User name</b> empty.
<b>Alternate queue manager</b>	(Optional) You can enter an alternate queue manager name that has been set up to forward its events to the primary queue manager specified above if you are also interested in monitoring those events.

GUI Element	Description
<b>Channel status code scheme</b>	<p>Select a reporting schemes for Channel Status Code values, and click <b>Apply</b>.</p> <ul style="list-style-type: none"> <li>▶ <b>Use HP coding scheme.</b> Report the actual or original channel status codes as documented in the IBM MQ literature.</li> <li>▶ <b>Use IBM MQ coding scheme.</b> Report channel status codes in ascending values that are directly proportional to the health of the channel. SiteScope reports a channel status value from 0 (least healthy) to 6 (healthiest). For details, see “Channel Status Codes” on page 1109.</li> </ul>
<b>Available Measurements</b>	<p>Displays available MQ queue instances and channel instances, and counters to choose from.</p> <p>In the <b>Objects</b> drop-down list, select either <b>Queue</b> or <b>Channel Objects</b> to work with. After an object is selected, a connection to the MQ server is made. A list of available queues or channels is displayed, both system and user instances, depending on the object type selected. Select the instances and counters you want to monitor, and click the <b>Add Selected Measurements</b>  button. The selected measurements are moved to the Selected Measurements list.</p>
<b>Selected Measurements</b>	<p>Displays the measurements currently selected for this monitor, and the total number of selected counters.</p> <p>To remove measurements selected for monitoring, select those measurements, and click the <b>Remove Selected Measurements</b>  button. The measurements are moved to the Available Measurements list.</p>



# 101

---

## WebSphere Performance Servlet Monitor

This chapter includes the main concepts and reference information for the WebSphere Performance Servlet monitor.

### **This chapter includes:**

#### Concepts

- WebSphere Performance Servlet Monitor Overview on page 1113

#### Reference

- WebSphere Performance Servlet Monitor Settings on page 1115

### **WebSphere Performance Servlet Monitor Overview**

Use the WebSphere Performance Servlet Monitor to monitor the server performance statistics for IBM WebSphere 3.0x, 3.5, 3.5.x, 4.0, 5.0, 5.1, 5.1.1, 6.0, 6.0.1, 6.0.2, 6.1, and 7.0 servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate WebSphere Performance Servlet Monitor instance for each WebSphere Application Server in your environment.

This section also includes:

- “Setup Requirements” on page 1114
- “Configuring the Monitor” on page 1115

## Setup Requirements

The following are several key requirements for using the WebSphere Performance Servlet Monitor:

- ▶ The WebSphere Performance Servlet is an optional component for WebSphere 3.0x and 3.5x versions. The performance servlet must be installed on WebSphere servers to use this monitor. A patch needs to be applied according to which WebSphere 3.x version you are monitoring.
- ▶ The WebSphere Performance Servlet must be installed on each WebSphere 3.x server you want to monitor. The files should be copied to the **hosts\default\_host\default\_app\servlets** subdirectory on each WebSphere server machine. The files needed per version are as follows:

Version	Files
3.02	xml4j.jar performance.dtd perf.jar
3.5	perf35.jar
3.5.2, 3.5.3	perf35x.jar

- ▶ The WebSphere Performance Servlet included as part of WebSphere 4.0 must be deployed. If you are running WebSphere 4.0 servers, only one instance of the servlet needs to be deployed to monitor one or more WebSphere 4.0 servers.
- ▶ Verify that the servlet is running properly and that the performance data is generated. One way to do this is to try to display it through an XML enabled browser. The servlet URL should be in the following format:

`http://<server:port>/<dir_alias>/com.ibm.ivb.epm.servlet.PerformanceServlet`

For example,

`http://wbs.company.com:81/servlet/com.ibm.ivb.epm.servlet.PerformanceServlet`

## Configuring the Monitor

For details on configuring the monitor, see “WebSphere Performance Servlet Monitor Settings” on page 1115.

## WebSphere Performance Servlet Monitor Settings

<b>Description</b>	<p>The WebSphere Performance Servlet Monitor to monitor the server statistics of IBM WebSphere Server by using a WebSphere Performance Servlet. The error and warning thresholds for the monitor can be set on one or more performance statistics.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “WebSphere Performance Servlet Monitor Overview” on page 1113</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## WebSphere Performance Servlet Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>Server</b>	Enter the server you want to monitor. On UNIX servers, enter the full path of the server.
<b>Secure server</b>	Select if the server being monitored is secure. <b>Default value:</b> Not selected
<b>Target</b>	Enter the logical name of the server that is the target of this monitor instance. Depending on the deployment of the WebSphere application in your infrastructure, this may be the same as the <b>Server</b> selected above. <b>Default value:</b> Empty (the host name is used)
<b>Port</b>	Enter the port number to the WebSphere server you want to monitor.
<b>Servlet URL</b>	URL of the performance servlet. For WebSphere versions 3.x.x, the URL can be viewed by using the Servlet Properties page in the WebSphere Admin Console. For WebSphere 4.0, the default URL is /wasPerfTool/servlet/perfservlet. In earlier versions, the URL is chosen during the installation of the servlet. For WebSphere 6.0 and later, use the URL: /wasPerfTool/servlet/perfservlet?version=5. In either case, the URL can be found in the Servlet properties page of the Admin Console.
<b>User name</b>	Enter the user name if the URL requires authorization.
<b>Password</b>	Enter the password if the URL requires authorization.

GUI Element	Description
<b>Advanced Settings</b>	
<b>Timeout (seconds)</b>	Enter the time, in seconds, that the monitor should wait for a response from the Performance Servlet. If a response is not received within the interval of the timeout, the monitor reports a timeout error. <b>Default value:</b> 60 seconds
<b>Refresh frequency</b>	Select a time interval at which the WebSphere server should update the metrics that are requested by this monitor. This value should be equal to or less than the <b>Frequency</b> time interval for the monitor in Monitor Run Settings. <b>Default value:</b> 10 minutes
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	The name of the proxy server if required.
<b>Proxy user name</b>	If the proxy server requires a name and password to access the server, enter the name here. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy password</b>	If the proxy server requires a name and password to access the server, enter the password here.
<b>WebSphere Performance Counters</b>	
<b>Counters</b>	The server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor. <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.



# 102

---

## XML Metrics Monitor

This chapter includes the main concepts and reference information for the XML monitor.

**This chapter includes:**

**Concepts**

- ▶ XML Metrics Monitor Overview on page 1120

**Reference**

- ▶ XML Metrics Monitor Settings on page 1122

## XML Metrics Monitor Overview

Use the XML Metrics monitor to monitor metrics for systems that make performance data available in the form of an XML file or page. The XML Metrics monitor gathers information from a source, organizes it into a browsable tree structure, and enables you to choose which items in the tree should be monitored. It works by requesting an XML file that is accessible by an URL. When the monitor runs, the XML metrics file is parsed to extract values for each of the counters selected during setup.

The XML metrics must be in a format where each metric is a separate, unique entity in the tree/leaf format. An optional XSL facility can help with formatting.

This section also includes:

- ▶ “XML Requirements” on page 1120
- ▶ “Configuring the Monitor” on page 1121

### **XML Requirements**

A monitor instance must be defined and run against the same XML metrics file format. That is, when running this monitor, SiteScope expects the XML file it is monitoring to have the same format that was used when defining that monitor.

SiteScope parses the input XML content according to the following assumptions:

- ▶ The XML content has only one root node. This means that all of the XML content is encapsulated within a single parent element and not multiple instances of a repeating root element.
- ▶ A leaf node, an element containing only character data and no child elements, is considered a counter and must be of the form:

```
<node_tag>node_value</node_tag>
```

where `<node_tag>` becomes the counter name, and `<node_value>` is reported as the counter value.



- Each leaf node (and therefore each counter) must have a unique path within the hierarchy of the XML content.
- The XML metric file should contain at least one leaf node.

If your XML metric file does not conform to these rules, you can specify an XSLT (eXtensible Stylesheet Language: Transformations) file that transforms your XML file into a file that does conform. Such a file usually has a file extension of .xsl.

If you need to develop a XSLT file to transform the XML content for this monitor, SiteScope includes a Tools page you can use to verify the transformation output. For more information, see the section “XSL Transformation Tool” on page 258.

### **Configuring the Monitor**

For details on configuring the monitor, see “XML Metrics Monitor Settings” on page 1122.



## XML Metrics Monitor Settings

<p><b>Description</b></p>	<p>The XML Metrics monitor enables you to monitor metrics for systems that make performance data available in the form of an XML file or page. The error and warning thresholds for the monitor can be set on one or more different objects.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ When deploying this monitor using a template, an error message is displayed if you clear the <b>Verify monitor properties with remote server</b> check box in the Deployment Values dialog box.</li> <li>▶ The <b>XSL Transformation Tool</b> is available when configuring this monitor to test a user defined XSL file that can be used to transform an XML file or output (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “XSL Transformation Tool” on page 258.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Deploy a Monitor – Workflow” on page 323</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “XML Metrics Monitor Overview” on page 1120</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## XML Metrics Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>XML URL</b>	Enter the URL of the XML page or file that contains the metrics that you want to monitor.
<b>XSL file</b>	Convert the XML metrics file into a format that SiteScope can use.
<b>Authorization NTLM domain</b>	Enter the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL.

GUI Element	Description
<b>Pre-emptive authorization</b>	<p>Select when the Authorization user name and Authorization password should be sent if SiteScope requests the target URL.</p> <ul style="list-style-type: none"> <li>▶ <b>Use global preference.</b> Select to have SiteScope use the authenticate setting as specified in the Pre-emptive authorization section of the General Preferences page. This is the default value.</li> <li>▶ <b>Authenticate first request.</b> Select to send the user name and password on the first request SiteScope makes for the target URL. <ul style="list-style-type: none"> <li><b>Note:</b> If the URL does not require a user name and password, this option may cause the URL to fail.</li> </ul> </li> <li>▶ <b>Authenticate if requested.</b> Select to send the user name and password on the second request if the server requests a user name and password. <ul style="list-style-type: none"> <li><b>Note:</b> If the URL does not require a user name and password, this option may be used.</li> </ul> </li> </ul> <p>All options use the <b>Authorization user name</b> and <b>Authorization password</b> entered for this monitor instance. If these are not specified for the individual monitor, the <b>Default authentication user name</b> and <b>Default authentication password</b> specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p><b>Note:</b> Pre-emptive authorization does not control if the user name and password should be sent, or which user name and password should be sent.</p>
<b>Timeout (seconds)</b>	<p>The number of seconds that the monitor should wait the XML page to complete downloading before timing-out. Once this time period passes, the monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 60 seconds</p>

GUI Element	Description
<b>Authentication Settings</b>	
<b>Authorization user name</b>	If the URL with the XML content you want to monitor requires a user name and password to access it, enter the user name.
<b>Authorization password</b>	If the URL with the XML content you want to monitor requires a name and password for access, enter the password.
<b>Proxy server</b>	If you must use a proxy server to access the XML URL, enter the host or domain name and port of the proxy server.
<b>Proxy server user name</b>	If you use a proxy server and the proxy requires a name and password to access the target URL, enter the user name. <b>Note:</b> The proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	If you use a proxy server and the proxy requires a name and password to access the target URL, enter the password. <b>Note:</b> The proxy server must support Proxy-Authenticate for these options to function.
<b>Accept untrusted certificates for HTTPS</b>	Select this option if you need to use certificates that are untrusted in the cert chain to access the target XML URL using Secure HTTP (HTTPS). <b>Default value:</b> Not selected
<b>Accept invalid certificates for HTTPS</b>	Select this option if you need to accept an invalid certificate to access the target XML URL using Secure HTTP (HTTPS). This may happen, for example, if the current date is not in the date ranges specified in the certificate chain. <b>Default value:</b> Not selected

GUI Element	Description
<b>Counter Settings</b>	
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.  <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.

# Part IV

---

## Integration Monitors





# 103

---

## Working with SiteScope Integration Monitors

Integration Monitors enable you to capture and forward data from several Enterprise Management Systems (EMS) applications and servers into HP Business Availability Center.

### **This chapter includes:**

#### **Concepts**

- ▶ Integration Monitors Overview on page 1130
- ▶ Topology Settings for Technology Integration Monitors on page 1133

#### **Tasks**

- ▶ Deploy Integration Monitors on page 1140

#### **Reference**

- ▶ List of Deprecated Integration Monitors on page 1142

**Troubleshooting and Limitations** on page 1143

## Integration Monitors Overview

Integration Monitors are run by the SiteScope data collector and are used to integrate data from third-party applications (typically EMS systems) into HP Business Availability Center.

---

**Note:** Access to Integration Monitor types requires that a special SiteScope Optional License be entered on the SiteScope server.

---

You can create an EMS integration in HP Business Availability Center's EMS Integrations Administration page. For details, see "EMS Integration Administration" on page 521 in the HP Business Availability Center Documentation Library. When creating the integration, the step to create monitors opens System Availability Management to enable you to create the SiteScope Integration monitors.

There are two levels of configuration for collecting the data and forwarding that data to HP Business Availability Center:

- ▶ **Required:** The monitors must be configured to properly map to the monitored system and collect the required samples, whether in the form of events, measurements, or tickets. The field mapping from the monitored system is done by selecting a sample type in the Field Mapping setting and editing the corresponding script template in a text editor.
- ▶ **Optional:** The data can also be mapped to a topology to forward data to the correct CI hierarchy in HP Business Availability Center. This enables the monitor to accurately report status to the required CIs within HP Business Availability Center for use by the different applications in the product. The topology settings are configured using a Jython script that is loaded depending on the type of topology you want to create.

This section includes the following topics:

- ▶ "Integration Monitor Categories" on page 1131
- ▶ "Field Mapping Sample Types" on page 1132

## Integration Monitor Categories

Integration monitors can be divided into two categories.

### Application-Specific Monitors

These integration monitors are designed for use with specific EMS applications. These monitors are predefined with the required field mapping and topology settings.

The monitors include:

- ▶ HP OVO Event Monitor
- ▶ HP Service Center Monitor
- ▶ NetScout Event Monitor

The scripts for both the field mapping and the topology settings can be further configured to suit the needs of your specific environment.

---

**Note:** Topology Settings are not available for the NetScout Event Monitor.

---

### Generic Integration Monitors

Technology Integration Monitors designed for use with most EMS applications that support extraction of data from a database, log file, SNMP trap, or Web service interface.

The field mapping and topology settings for these monitors must be configured by loading the applicable scripts and editing them in a separate text editor during monitor creation.

The monitors include:

- ▶ Technology Database Integration Monitor
- ▶ Technology Log File Integration Monitor
- ▶ Technology SNMP Trap Integration Monitor
- ▶ Technology Web Service Integration Monitor

## Field Mapping Sample Types

The integration monitors use field mapping scripts to correctly map the data they collect to a format recognizable by HP Business Availability Center. For the generic integration monitors, you configure and customize these mappings as required. When you select a field mapping type, you must copy the script into a text editor, make your changes, and then copy the script back into the field mapping text box.

The mappings for the application-specific monitors are not editable while configuring the monitor and we recommend that you use the out-of-the-box integration mappings already configured for those monitors.

When configuring the generic integration monitors, select from the following types of sample scripts:

- ▶ **Measurements.** Used to collect time-based data. Data collected by Integration Monitors that use the measurements sample type is integrated into HP Business Availability Center as typical SiteScope data and can be viewed in all contexts that support viewing SiteScope data (for example, Dashboard, Service Level Management, System Availability Management, user reports, and so on).
- ▶ **Events.** Used to collect data on specific events. Data collected by Integration Monitors that use the event sample type is integrated into HP Business Availability Center using the UDX framework and can be viewed in contexts that support the display of UDX data (Event Log, Dashboard, trend reports). The data can also be accessed using the HP Business Availability Center API.
- ▶ **Tickets.** Used to collect incidents and events from ticketing systems. Data collected by integration monitors that use the ticketing sample type is integrated into HP Business Availability Center and can be viewed in Dashboard and Service Level Management.

The Database, Log File, SNMP Trap, and Web Service Technology Integration Monitors can be configured to work with these sample types. You use the field mapping script templates that come prepackaged with SiteScope as a basis for creating a customized configuration required for your specific environment. When you configure an integration monitor, you select the sample type to load the required script template and edit the script to collect the data you want to forward to Business Availability Center.

For details on customizing the field mapping scripts, see “Integration Monitor Field Mapping” on page 1147.

## **Topology Settings for Technology Integration Monitors**

To establish the full integration with Business Availability Center, you can select a topology template for your integration monitor. You do this while creating an integration monitor in the Topology Settings area. The topology templates for **Hosts**, **Hosts-Software Elements**, and **Tickets** are specially configured with the necessary values to forward data to the required CIs in Business Availability Center’s CMDB.

The topology is written as a Jython script. Jython is a language based on Python and powered by Java. For details on how to work in Jython, you can refer to these Web sites:

- <http://www.jython.org>
- <http://www.python.org>

The script includes the basis of the functions necessary to retrieve the required topology data from the monitored application. To build the topology, the script uses the sample that was created as a result of the monitor’s field mapping. The script includes the mapping to forward the retrieved data to the relevant CIs in Business Availability Center.

SiteScope forwards the topology to create or update a CI under the following conditions:

- When the CI is created in SiteScope for the first time as a result of the monitor retrieving data, regardless of whether the CI exists in the CMDB.
- If there were any changes to any of the CI’s properties.
- The initial monitor run after SiteScope is restarted.

This prevents overloading the CMDB with CI updates coming from the monitor.

This section includes the following topics:

- “Selecting a Topology” on page 1134
- “Editing the Topology Script” on page 1137
- “Jython Properties File” on page 1139

## Selecting a Topology

When working with application-specific monitors, you do not select a topology and the topology is preconfigured with the necessary data for the integration.

When working with generic integration monitors, you can select from the following topology settings:

- **Custom.** You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or software element CIs.

---

**Note:** It is recommended not to select **Custom** as this does not load a script and you must enter the entire script yourself. We recommend that you begin with either **Hosts** or **Hosts-Software Elements** and edit one of those scripts.

---

- **Hosts.** Creates a host CI with an EMS monitor CI as a leaf node.
- **Hosts-Software Element.** Creates a topology with a host CI as the parent CI and a software element CI under it, and an EMS monitor CI under the software element CI.
- **Tickets.** Creates a business service CI with an EMS monitor CI as a leaf node.

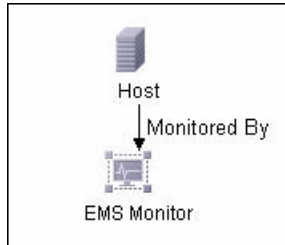
---

**Note:** The topology script must include the EMS monitor CI as the lowest leaf in the topology created by the integration.

---

## Hosts Topology

The default topology created includes a Host CI with an EMS Monitor CI as its leaf node.



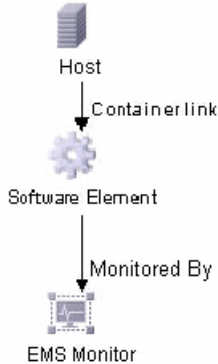
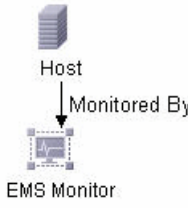
The Host CI has a monitored by relationship with the EMS Monitor CI. The EMS Monitor CI passes status onto the Host CI.

## Hosts-Software Elements Topology

In this topology, there are two types of data that can be retrieved from the monitored system: **software element** events and **system** events.

- **Software element events.** This data is recognized as data affecting services or applications. These events are mapped to the system KPI for the relevant CIs. These events are not propagated to the host CIs.
- **System events.** This data is all other data retrieved from the monitored application that does not affect services or applications. This data passes status onto the host CI. The status may propagate to the Application CI if there is a relationship between the host CI receiving the system event and the software element CI. This event is also mapped to the system KPI for the relevant CIs.

The following table illustrates the topology created for each type of event:

Topology Created for Software Element Event	Topology Created for System Event
 <pre> graph TD     Host[Host] -- Container link --&gt; SE[Software Element]     SE -- Monitored By --&gt; EMS[EMS Monitor]             </pre>	 <pre> graph TD     Host[Host] -- Monitored By --&gt; EMS[EMS Monitor]             </pre>

If the events do not belong to the category of service events, then the event is considered a system event.

You can configure which data is considered application or service data and which data is not. You configure these instructions by editing the topology script as follows:

Search for the following string in the topology script:

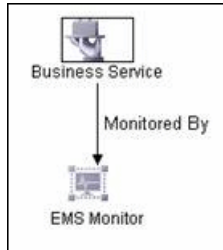
**if (subject != "system"):**

The variable **subject** represents the subject field in the retrieved sample (as defined in the field mapping for events). The value **system** is an example of possible values representing the data from an application that is considered 'system' data and not forwarded to the software element CI. This 'system' data is forwarded to the host CI.



## Tickets

The default topology created includes a Business Service CI with an EMS Monitor CI as its leaf node. The Business Service CI has a monitored by relationship with the EMS Monitor CI.



The EMS Monitor CI passes status onto the Business Service CI.

## Editing the Topology Script

To configure the topology, you must edit the Jython script that appears in the Topology Settings area when creating an integration monitor. We highly recommend that you copy the contents of the script into your preferred text editor, edit the script in the text editor, and then copy back the contents into the Topology Settings field for the monitor.

The **Hosts**, **Hosts-Software Elements**, and **Tickets** topologies are already configured with the necessary information. Following are the guidelines for editing the script if you want to create your own topology.

- We recommend that you familiarize yourself with the Jython language before attempting to edit this script.
- The Jython language is sensitive to spaces and tabs and you must be careful while editing the script.
- You must leave the import section as is and only add to it.
- The main body of the script is mandatory and consists of:

```
def DiscoveryMain(Framework)
```

This main function is responsible for creating Object State Holder Vector (OSHV) results. This holds the CI data and how to map the incoming samples to the CIs.

- ▶ Each CI should have only one EMS Monitor CI as a leaf node.
- ▶ For event scripts, the following expressions must appear as the last lines in the script:

```
Framework.setUserObject("result_object",monitoredCiType)
return OSHVResult
```

The variable `monitoredCiType` is the CI type being monitored by the EMS Monitor CI that receives the event.

If the script creates more than one EMS Monitor CI for one retrieved event, you must determine to which of the CIs that event belongs and passes status. You do this by assigning the correct value to the `monitoredCiType`. For example, if the script creates one EMS Monitor CI for an Application CI and one for a Host CI, and you want the event to pass status to the Host CI, the value of the variable `monitoredCiType` should be "host".

- ▶ Use the built-in "logger" to debug the topology scripts when samples arrive. You do this by modifying the level and type of information reported to the log file. Change the log file settings in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties** file as follows:

- a** Open the **log4j.properties** file in a text editor and locate the following lines in the file:

```
# Jython prints
log4j.category.PATTERNS_DEBUG=${loglevel}, integration.appender
```

Change the argument of **log4j.category.PATTERNS\_DEBUG** from **`\${loglevel}** to **DEBUG**, as follows:

```
log4j.category.PATTERNS_DEBUG=DEBUG, integration.appender
```

- b** Save the file. It may take a few seconds for the changes to take effect.

The results are logged to the **bac\_integration.log** file.

## Jython Properties File

The <SiteScope root directory>\conf\ems\jython.properties file controls many aspects of the Jython script. Generally, you do not need to edit this file. It already includes all the properties necessary for running the Jython script.

If you working in a secure Business Availability Center installation that has a certificate, you may have to modify one of the properties in this file. In this case, you must insert the following line into the file:

```
appilog.agent.Probe.BasicAuth.Realm=MyPrivateFile
```

Where myPrivateFile is a variable for the certificate realm. If you want to find out what realm a given URL belongs to, you can open the URL with a Web browser and see the first line in the popup box.

---

**Note:** When you modify the **jython.properties**, you must restart SiteScope to enable your changes to take effect.

---

## Deploy Integration Monitors

This task describes the steps involved in deploying an integration monitor.

You can deploy integration monitors while working in:

- ▶ Business Availability Center’s EMS Integrations Administration which opens System Availability Management Administration
- ▶ Directly in System Availability Management Administration
- ▶ A standalone SiteScope that reports to Business Availability Center

This task includes the following steps:

- ▶ “Select a SiteScope” on page 1140
- ▶ “Create a Group for the Integration Monitor” on page 1140
- ▶ “Configure the Integration Monitor” on page 1141
- ▶ “Edit Field Mappings and Topology Script” on page 1141

### 1 Select a SiteScope

When in System Availability Administration, select the SiteScope server from which you want to deploy the integration monitor. For details on the user interface, see “System Availability Management Administration” on page 125.

---

**Note:** This step is relevant only for users accessing SiteScope from HP Business Availability Center.

---

### 2 Create a Group for the Integration Monitor

We recommend that you create special groups for the integration monitors. This enables you to more easily recognize the data that is reported to Business Availability Center as coming from the integrations.

For details on the New SiteScope Group user interface, see “New SiteScope Group Dialog Box” on page 297.

### 3 Configure the Integration Monitor

You must configure the monitor and add the required data for the monitor's settings. You can choose from the following application-specific integrations:

- HP OVO Event Monitor
- HP Service Center Monitor
- NetScout Event Monitor

You can choose from the following generic integration monitors:

- Technology Database Integration Monitor
- Technology Log File Integration Monitor
- Technology SNMP Trap Integration Monitor
- Technology Web Service Integration Monitor

### 4 Edit Field Mappings and Topology Script

For generic integration monitors or any special customizations, you must also:

- Edit the field mappings. For details on this topic, see “Integration Monitor Field Mapping” on page 1147.
- Edit the topology settings. For details on this topic, see “Topology Settings for Technology Integration Monitors” on page 1133.

## List of Deprecated Integration Monitors

In SiteScope version 8.5, a number of Integration Monitors were deprecated and are no longer supported.

The following table lists the deprecated Integration Monitors, and the respective Technology Integration Monitors that can replace them:

Deprecated Monitor	Recommended Monitor
Avalon Event	Technology SNMP Trap
BMC Patrol Event	Technology SNMP Trap, Technology Log File
BMC Patrol	Technology Log File
CA Unicenter Event (1)	Technology SNMP Trap
Compaq Insight Manager Event (2)	Technology Database
HP Systems Insight Manager Event	Technology Database
Netcool Event	Technology SNMP Trap
NetIQ (3)	Technology Database
Remedy Ticketing	Technology Database
Tivoli TEC Event	Technology Database
Tivoli DM	Technology Database
WhatsUp Event (4)	Technology Log File

The following are examples of how a Technology monitor can be configured to replace a deprecated monitor:

(1) Configure CA Unicenter agents to send SNMP traps to a SiteScope host machine where a Technology replacement monitor has been configured.

(2) For Compaq Insight Manager version 7.0, configure the replacement SiteScope monitor to read from the following tables: Notices, NoticeType, Devices, StringResource, and StringTableLarge.

(3) For NetIQ versions 5.0 and 5.1, configure the replacement SiteScope monitor to query tables **Data** (contains raw data) and **DataHeader** (contains metadata about the objects that NetIQ monitors).

(4) For WhatsUp version 8.0, configure the replacement SiteScope monitor to read from the log file **EV-<date>.tab**.

---

**Note:** Beginning with SiteScope 8.x, the monitor configuration file **main.config** is no longer used. All functions that were supported in **main.config** are now supported in **event.config** and available in the **Fields Mapping** setting.

---

## Troubleshooting and Limitations

The information below describes basic troubleshooting techniques and information regarding log files that may be useful when working with Integration Monitors.

### Integration Monitor Logs

Integration Monitor activity is logged to **<SiteScope root directory>\logs\RunMonitor.log** and **lbac\_integration.log**.

You can modify the level and type of information reported to the log file by changing the log file settings in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties** file. You can instruct the logging mechanism to:

- ▶ report logged information in less or greater detail than is reported by default
- ▶ log all samples sent by Integration Monitors to HP Business Availability Center
- ▶ log all received events from external EMS systems

**To modify log settings:**

- 1** Open the **log4j.properties** file in a text editor.
- 2** To specify that samples sent by Integration Monitors to HP Business Availability Center be logged:
  - a** Locate the following lines in the file:

```
log4j.category.EmsSamplePrinter=${loglevel}, integration.appender  
log4j.additivity.EmsSamplePrinter=false
```
  - b** Change the argument of **log4j.category.EmsSamplePrinter** from **\${loglevel}** to **DEBUG**, as follows:

```
log4j.category.EmsSamplePrinter=DEBUG, integration.appender
```
  - c** Save the file. It may take a few seconds for the changes to take effect.The results are logged to the **bac\_integration.log** file.

- 3** To specify that all received events from external EMS systems be logged:
  - a** Locate the following lines in the file:

```
log4j.category.EmsEventPrinter=${loglevel}, monitors.appender  
log4j.additivity.EmsEventPrinter=false
```
  - b** Change the argument of **log4j.category.EmsEventPrinter** from **\${loglevel}** to **DEBUG**, as follows:

```
log4j.category.EmsEventPrinter=DEBUG, monitors.appender
```
  - c** Save the file. It may take a few seconds for the changes to take effect.The results are logged to the **RunMonitor.log** file.

**Other Log and Troubleshooting Issues**

- Look for errors in **<SiteScope root directory>\logs\error.log** and in **<SiteScope root directory>\logs\bac\_integration.log**.
- If samples are created and sent from SiteScope but cannot be seen in HP Business Availability Center Dashboard, Event Log, or SiteScope reports, search for the string **ERROR** or **WARN** in the **wde.logl** and **loader.logl** files in the **<HP Business Availability Center root directory>\log\mercury\_wde\** directory to make sure the samples were not dropped due to missing fields or values.



- Increase the level of Dashboard logging in <HP Business Availability Center root directory\conf\core\Tools\log4j\EJB\ble.properties file to verify that Dashboard is receiving samples. Locate the following parameter and change the log level status to **DEBUG**:

```
log4j.category.Trinity.BLE_SAMPLES=DEBUG, trinity.samples.appender
```

The results are logged to the <HP Business Availability Center root directory\log\EJBContainer\TrinitySamples.log.

---

**Note:** Once you have determined the cause of the problem, we recommend that you set log levels to their default settings so as not to overload the system.

---

Additional troubleshooting information is located in the HP Software Self-solve knowledge base (<http://h20230.www2.hp.com/selfsolve/documents>) (you must log in to the knowledge base with your HP Passport ID) and in the following sections of the documentation:

- For Technology Database Integration monitor, see “Troubleshooting the Technology Database Integration Monitor” on page 1223.
- For Technology Log File monitor, see “Troubleshooting the Technology Log File Integration Monitor” on page 1240.
- For Technology SNMP Trap monitor, see “Troubleshooting the Technology SNMP Trap Integration Monitor” on page 1253.
- For Technology Web Service Integration monitor, see “Troubleshooting the Technology Web Service Integration Monitor” on page 1267.



# 104

---

## Integration Monitor Field Mapping

You enable capturing event and metrics data from Enterprise Management Systems, automated support systems, and other management applications by configuring integration monitors and their field mapping scripts.

### **This chapter includes:**

#### **Concepts**

- Integration Monitor Field Mapping Overview on page 1148
- Understanding Field Mapping Structure on page 1149

#### **Reference**

- Configuring Field Mapping for Event Samples on page 1150
- Configuring Field Mapping for Measurement Samples on page 1156
- Configuring Field Mapping for Ticket Samples on page 1159
- Event Handler Structure on page 1163

## Integration Monitor Field Mapping Overview

Integration monitors depend on field mappings you customize within the user interface in the settings for the monitor. The mapping defines the processing of incoming data and defines the output sample forwarded to Business Availability Center.

Integration Monitors designed for use with specific EMS applications (these currently include HP OVO, HP Service Center, and NetScout) can be configured without editing their field mapping script. The mappings are predefined by HP and require modification only if specific customizations are required. For details on editing these field mapping scripts, see the description for the field mapping element in the user interface pages for the monitor you are deploying.

For Technology Integration Monitors (Technology SNMP Trap, Technology Log File, and Technology Database monitors), you must select the sample type and the required script template is loaded directly into the field mapping text box. You must edit the field mapping script to suite your organization's needs. The Technology Web Service Integration Monitor field mapping may also need to be customized. You can select from the following sample types:

- ▶ **Events.** Select to forward event data to Business Availability Center.  
When you select **Events** and you want to integrate to Business Availability Center using topology settings, it is recommended that you select from the following topology script templates: **Hosts** or **Hosts-Applications**.
- ▶ **Measurements.** Select to forward measurement data to Business Availability Center.  
When you select **Measurements**, it is recommended not to select a topology script. If you do, the script may fail.
- ▶ **Tickets.** Select to forward ticket data to Business Availability Center.  
When you select **Tickets** and you want to integrate to Business Availability Center using topology settings, it is recommended that you select the following topology script template: **Tickets**.

For details, on selecting a topology setting, see “Topology Settings for Technology Integration Monitors” on page 1133.

---

**Note:** Use only the mandatory and optional fields defined in the script templates when working with the field mapping. For more information, see the tables for each sample type.

---

## Understanding Field Mapping Structure

The field mapping contains instructions on how to process the data as it arrives to the integration monitors. The instructions that constitute the field mappings are grouped into event handlers—independent sections that contain instructions relevant to specific data. Each event handler contains a **matching condition** by which SiteScope can determine whether to use a particular event handler for an arriving event.

When an event or measurement data arrives at the integration monitor, it iterates over the different event handlers in the field mapping, in the order they appear, testing the **matching condition** of each handler. If a matching handler is found, the monitor uses the instructions within that handler to process the event and perform the action defined for this handler (for example, forward it to Business Availability Center or discard). No further sections are checked after the first match. If no matches are found, the event is discarded.

In addition to the event handlers, the field mapping can contain special entries that affect the integration monitor engine as a whole. These values are grouped into the `[$DEFAULT_PARAMETERS$]` section. This section defines default values for tags that are common for all handlers. Any tag can be set in this section of the field mapping. It is used to create a reported value unless overridden in the matched event handler. For each incoming event, this event handler is always run prior to the matched event handler.

For details on event handler structure, see “Event Handler Structure” on page 1163.

## **Configuring Field Mapping for Event Samples**

The events sample type is used for extracting events collected by external systems and importing them to Business Availability Center. When configuring an integration monitor's field mapping, select the **Events** sample type to load the events script. You can then copy the contents of the **Field Mapping** text box and paste it into a text editor to make your configuration changes. When you are done, copy the contents back into the Field Mapping text box.

This section includes the following topics:

- “Mandatory Values for the Event Script” on page 1151
- “Optional Values for the Event Script” on page 1152
- “Conditional Expression Example 1” on page 1154
- “Conditional Expression Example 2” on page 1154
- “Event Script Example” on page 1155

## Mandatory Values for the Event Script

The table below lists mandatory values for the event script.

Field Name	Type	Description	Example
time_stamp	DOUBLE	Time stamp in seconds since Jan 1 1970.	time_stamp:DOUBLE=str_to_seconds(\$time,"yyyy-MM-dd HH:mm:ss.SSS"). time_stamp:DOUBLE=time()
severity	INT	Can be one of the following preconfigured severities (based on applicable integer): 0:SEVERITY_UNKNOWN 1:SEVERITY_INFORMATIONAL 2:SEVERITY_WARNING 3:SEVERITY_MINOR 4:SEVERITY_MAJOR 5:SEVERITY_CRITICAL	severity:INT=SEVERITY_MINOR
target_name	STRING	Name of device or host that generated the event.	target_name=\$hostName target_name=resolveHostName (String host name)
status	STRING	Status of event in external EMS terminology.	status="OPEN" status="ASSIGNED" status="CLOSED"
subject	STRING	Subject of event (e.g. CPU, SAP application, Hard Disk), middle/high level hierarchy describing the event source.	subject="DISK"

Field Name	Type	Description	Example
instance	STRING	Instance of subject that generated the event (e.g D:\). Lowest level of hierarchy describing the event source.	instance="E:\\"
description	STRING	Textual description of event.	description="free space on drive e is below 10%"
data_source	STRING	System that generated the event.	data_source="HP OVO"

### Optional Values for the Event Script

The table below lists optional values for the event script.

Field Name	Type	Description	Example
target_ip	STRING	IP of host or device that generated the event.	target_ip=\$IPString
object	STRING	Optional level in the hierarchy describing the event source.	object="OS"
event_id	STRING	Unique identifier of this event.	event_id=\$id
logical_group	STRING	Logical grouping of this event.	logical_group="error messages"
monitor_group	STRING	Monitor group that reported this event.	monitor_group="log monitors on \\hostname"
orig_severity_name	STRING	Severity in external EMS terminology.	orig_severity_name="Cleared"
acknowledged_by	STRING	Name of user that acknowledged this event.	acknowledged_by=\$username



Field Name	Type	Description	Example
owner	STRING	Name of user who owns this event.	owner="admin"
value	DOUBLE	Use to transfer numerical values from the event.	value=\$thresholdViolated
attr1	STRING	Extra data slot.	attr1=\$history
attr2	STRING	Extra data slot.	attr2=\$moreHistory
attr3	STRING	Extra data slot.	attr3="Design"
attr4	STRING	Extra data slot.	attr4=\$MonitorOutput
attr5	STRING	Extra data slot for long strings.	attr5=\$Longhistory

### Host DNS Resolution for Event Sample

Both the FQDN (fully qualified domain name) and valid IP address are necessary for the fields that are used to create host CIs in HP Business Availability Center integration.

If you do not know the FQDN and/or IP address, then you can use the following functions in the field mapping to resolve the names and access them from the source of the integration:

**target\_name=resolveHostName(\$SomeHost)**

**target\_ip=resolveHostIP(\$SomeHost)**

---

**Note:** The variable **\$SomeHost** must be replaced by a variable from the integration source.

---

These functions are not necessary if:

- ▶ The FQDN and/or IP address is available from the source that the integration is accessing. In this case, you should input the value for **target\_name=** as a FQDN and the value for the **target\_ip=** without the function.
- ▶ It is not possible for the SiteScope server to resolve the FQDN and/or IP address for the servers from the source that the integration is accessing. In this case, the functions may not provide the valid values.

### Conditional Expression Example 1

```
severity:INT=$var6.equals("red") ? SEVERITY_CRITICAL  
: SEVERITY_INFORMATIONAL
```

In this example, the value of sixth variable binding is compared to string red. If the variable binding is indeed equal to string red, then the value of the severity tag is set to SEVERITY\_CRITICAL, otherwise it is set to SEVERITY\_INFORMATIONAL.

### Conditional Expression Example 2

```
severity:INT=$var6.equals("red") ? SEVERITY_CRITICAL :  
$var6.equals("green") ? SEVERITY_INFORMATIONAL : $var6.equals("yellow")  
? SEVERITY_MINOR : SEVERITY_WARNING
```

This example chains the conditional operator into a decision chain. If the sixth variable binding holds string red, then severity tag has the value SEVERITY\_CRITICAL. If the sixth variable binding holds string green, then severity tag has the value SEVERITY\_INFORMATIONAL. If the variable binding holds string yellow, the tag has the value SEVERITY\_MINOR. If none of the above conditions are true, then the tag has the value SEVERITY\_WARNING.

## Event Script Example

In the example below, two types of events are sent: the first are events of status "OPEN" and the second are events cleared by a user. The data is retrieved from incoming event fields using the \$ notation. All other events are discarded by the last handler.

```
[DEFAULT_PARAMETERS$]
#####
# NOTE: the following parameters are mandatory #
#####
time_stamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS")
severity:INT= SEVERITY_UNKNOWN
target_name=$Device
status=$Status
subject="EMS X Events"
instance=$target
description=$description
data_source="EMS X"

#send an open event with the value in value fields and with the event id
[OPEN events]
$MATCH="OPEN".equals($Status)
$ACTION=TOPAZ_BUS_POST(event)
value:DOUBLE=parseDouble($threshold)
event_id=$uid

#send clear events with the event id and acknowledging username
[clear events]
$MATCH="CLEAR".equals($Status)
$ACTION=TOPAZ_BUS_POST(event)
event_id=$uid
acknowledged_by=$ClearedBy

[event sink]
$MATCH=true
$ACTION=DISCARD
```

## **Configuring Field Mapping for Measurement Samples**

The measurements sample type is used for extracting metrics collected by external systems and importing them to Business Availability Center. When configuring an integration monitor's field mapping, select the **Measurements** sample type to load the measurements script. You can then copy the contents of the **Field Mapping** text box and paste it into a text editor to make your configuration changes. When you are done, copy the contents back into the Field Mapping text box.

This section includes the following topics:

- ▶ “Mandatory Values for the Measurements Script” on page 1157
- ▶ “Measurements Script Example” on page 1157

## Mandatory Values for the Measurements Script

The table below lists mandatory values for the measurements script.

Field Name	Type	Description	Example
TimeStamp	DOUBLE	Time stamp in the seconds since Jan 1st 1970 format.	TimeStamp:DOUBLE=time ()
Quality	INT	Quality in SiteScope terms. Possible values are: QUALITY_ERROR, QUALITY_WARNING, QUALITY_GOOD.	Quality:INT=QUALITY_ERROR
MonitorName	STRING	Logical monitor name.	MonitorName="NT cpu Monitor"
MonitorState	STRING	The monitor status, for example, N\A, Good, Error, and so on.	MonitorState="Received " + \$count + " events"
MonitorType	STRING	The monitor type.	MonitorType="System Monitor"
TargetName	STRING	The target of this monitor (e.g. host name).	TargetName=\$Device
Measurement Name(N)	STRING	Name the Nth measurement.	MeasurementName(1)="C PU Temperature"
Value(N)	DOUBLE	Value of Nth measurement.	Value(1):DOUBLE=\$CPU Temperature

## Measurements Script Example

In the example below, two measurements are sent: the first one (MeasurementName (1)) takes its name from the \$legend field and takes the value from the \$value field. A second measurement (Measurement Name (2)) uses the constant name CPU Temperature which receives its value from the \$CPUTemp field.

```
#####
#      EMS Integration metricsconfig file #
# use this file to send metrics to HP Business Availability Center #
#####
[$DEFAULT_PARAMETERS$]
# time stamp in the seconds since Jan 1st 1970 format.
TimeStamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS")

# quality in SiteScope terms QUALITY_ERROR, QUALITY_WARNING,
QUALITY_GOOD
Quality:INT=QUALITY_ERROR

# Logical monitor name
MonitorName=$kpName

#target, e.g. host name
TargetName=$parentMachineName

#the status string of the monitor (e.g.: "Log file read, 3 matches found")
MonitorState="The monitor status is: " + $status

#the monitor type (e.g. "Log Monitor", "CPU Monitor")
MonitorType="NetIQ measurements"

#measurement name
MeasurementName(1)=$legend
#value as double
Value(1):DOUBLE=parseDouble($value)

#measurement name
MeasurementName(2)="CPU Temperature"
#value as double
Value(2):DOUBLE=parseDouble($CPUTemp)
#####
# To send more than one measurement per DB row #
# add pairs #
# MeasurementName (*) = #
# Value (*) :DOUBLE= #
# where * = 1,2,..,n #
#####
[allR]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(ss_t)
```

When specifying more than one measurement in the script, a separate sample is sent with each of the measurements.

---

**Note:** When specifying multiple measurements per file, the measurement numbering must be consecutive.

---

In the case of failure, errors appear in the **RunMonitor.log** but the error does not affect the monitor status.

## **Configuring Field Mapping for Ticket Samples**

The ticket sample type is used for extracting events collected by external systems and importing them to Business Availability Center. When configuring an integration monitor's field mapping, select the **Tickets** sample type to load the tickets script. You can then copy the contents of the **Field Mapping** text box and paste it into a text editor to make your configuration changes. When you are done, copy the contents back into the Field Mapping text box.

This section includes the following topics:

- “Mandatory Values for the Ticket Script” on page 1160
- “Optional Values for the Ticket Script” on page 1161
- “Conditional Expression Example” on page 1162
- “Ticket Script Example” on page 1162

## Mandatory Values for the Ticket Script

The table below lists mandatory values for the ticket script.

Field Name	Type	Description	Example
time_stamp	DOUBLE	Time stamp in seconds since Jan 1 1970.	time_stamp:DOUBLE=str_to_seconds(\$time,"yyyy-MM-dd HH:mm:ss.SSS").
severity	INT	Can be one of the following preconfigured severities (based on applicable integer): SEVERITY_UNKNOWN SEVERITY_INFORMATIONAL SEVERITY_WARNING SEVERITY_MINOR SEVERITY_MAJOR SEVERITY_CRITICAL	4".equals(\$severity) ? "Low" : ("3".equals(\$severity) ? "Average" : ("2".equals(\$severity) ? "High" : ("1".equals(\$severity) ? "Critical" : "Unknown")))
target_name	STRING	Name of the entity (usually a service) that generated the ticket.	target_name="mail service" (Do not enter static string here, should be retrieved dynamically from the ticket.)
data_source	STRING	System that generated the ticket.	data_source="ticketing" (This string should not be edited for HP ServiceCenter integration and must be edited for a generic technology integration monitor.)
ticket_id	STRING	ID of the ticket.	ticket_id=112233
ticket_state	STRING	One of the states in the incident lifecycle as defined in the ticketing system.	"Open" / "Closed"



Field Name	Type	Description	Example
ticket_type	STRING	Type of the incident as defined in the ticketing system.	"Incident"
orig_severity_name	STRING	Severity in external EMS terminology.	orig_severity_name="Cleared"

### Optional Values for the Ticket Script

The script includes comments describing the optional values available for the ticket script. They include those listed here:

Field Name	Type	Description	Example
subject	STRING	Middle/High level hierarchy describing the event source.	CPU, SAP application, hard disk
instance	STRING	Instance of subject that generated the event. The lowest level hierarchy describing the event source.	D:\
object	STRING	Optional level in the hierarchy describing the ticket source.	object="OS"
logical_group	STRING	Logical grouping of this ticket.	logical_group="error messages"
monitor_group	STRING	Monitor group that reported this ticket.	monitor_group="log monitors on \\hostname"
elapsed_time	STRING	Elapsed time of the ticket.	
orig_severity_name	STRING	Severity name as defined in the ticketing system.	
attr1	STRING	Extra data slot.	attr1=\$history

Field Name	Type	Description	Example
attr2	STRING	Extra data slot.	attr2=\$moreHistory
attr3	STRING	Extra data slot.	attr3="Design"
attr4	STRING	Extra data slot.	attr4=\$MonitorOutput
attr5	STRING	Extra data slot for long strings. Use for values up to 2000 chars.	attr5=\$Longhistory

### Conditional Expression Example

```
4".equals($severity) ? "Low" : ("3".equals($severity) ? "Average" :
("2".equals($severity) ? "High" : ("1".equals($severity) ? "Critical" : "Unknown"))))
```

This example configures the severity of the ticket sample. It matches between the status terms used in the ticketing system to those used in Business Availability Center.

### Ticket Script Example

```
[$DEFAULT_PARAMETERS$]
time_stamp:DOUBLE=$time_stamp
ticket_id=$ticket_id
ticket_state=$ticketStatus
severity:INT=$severity
target_name=$target_name
data_source="ticketing"
ticket_type="Incident"
orig_severity_name="4".equals($severity) ? "Low" : ("3".equals($severity) ? "Average" :
("2".equals($severity) ? "High" : ("1".equals($severity) ? "Critical" : "Unknown"))))
```

## Event Handler Structure

Each event handler has following structure:

```
[name]
Matching condition
Action directive
Tags
```

The names of **Matching condition**, **Action directive**, and additional directives start with dollar sign symbol (\$). The names of tags should not start with dollar sign.

Comments are allowed in the field mapping. The comment starts with either #, !, or ; character and continues to the end of the line.

---

**Note:** Use only the mandatory and optional fields defined in the script templates when working with the field mapping. See the tables in the following sections for more information.

---

This section includes the following topics:

- “Matching Condition” on page 1164
- “Basic String Expressions” on page 1168
- “Basic Conditional Expression” on page 1168
- “Action Directive” on page 1168
- “Tags” on page 1169
- “Integration Monitor Field Mapping Examples” on page 1170

## Matching Condition

The Match Condition must be a valid boolean expression. The expression can contain calls to the operators and functions defined below. The expression can access the contents of the event that is being processed using the dollar sign (\$) notation. For example, if the incoming event is SNMP Trap, then its enterprise OID can be accessed as \$oid. For names specific to a monitor, refer to the documentation of the relevant monitor type.

---

**Note:** The Match Condition expression is limited to 4,000 characters.

---

The matching condition has the form:

```
$MATCH=Boolean expression
```

where the Boolean expression is one of the expressions listed in the table below. When mentioned in the description, the expression can also be used to assign values into tags (see “Tags” on page 1169).

Expressions and Functions	Description	Examples	True if
<, <=, >, >=, ==, !=	Checks the numerical correctness of the expression. Can be used with INT or DOUBLE fields.	\$MATCH=\$numberOfLines == 100	\$numberOfLines equals 100
		\$MATCH=\$numberOfColumns <= 107	\$numberOfColumns equals 107 or less
equals(String)	Checks for string equality.	\$MATCH="ERROR".equals(\$status)	\$status equals the word ERROR
		\$MATCH=\$status.equals("ERROR")	\$status equals the word ERROR

Expressions and Functions	Description	Examples	True if
true, false	Constant Boolean values.	\$MATCH= true	always true.
&&,	To be used to combine any of the above boolean expressions.	\$MATCH= \$status.equals ("ERROR")    \$numberOfLines == 100	\$status equals the word ERROR or if \$numberOfLines equals 100
time()	Returns the current time, in seconds, since January 1, 1970 format. Can be used with DOUBLE fields.	\$MATCH= \$timeStampField > (time()-600)	the value of the \$timeStampField is newer than ten minutes ago (in seconds, since January 1, 1970 format)
parseInt (String), parseDouble( String),	Use to convert strings to numeric values. The input string should be a valid representation of an integer or a floating point number.  <b>Note:</b> calling this function on a string that cannot be interpreted as a number causes an error and the incoming event is dropped.  Can also be used with INT or DOUBLE fields.	\$MATCH= parseInt(\$size) > 10	the string value in \$size is an integer larger than 10.

Expressions and Functions	Description	Examples	True if
str_to_seconds(Str1, Str2)	Calculates the timestamp (in seconds, since January 1, 1970 format) held in the first String using the format in the second string. Can also be used with DOUBLE fields.	<p><b>\$MATCH=</b>  str_to_seconds (\$time,"yyyy-MM-dd HH:mm:ss.SSS") &gt; time()</p> <p><b>Note:</b> use the following symbols to represent time:  Year - 'y'  Month - 'M'  Day of month - 'd'  Hour - 'H'  Minute - 'm'  Second - 's'</p>	<p>the date specified in \$time in yyyy-MM-dd HH:mm:ss.SSS format is later than the current time.</p> <p>For more information, search the Internet for SimpleDateFormat.</p>
exist(\$field)	Checks for an existence of a field in the processed event and make sure that it is not an empty value.	<b>\$MATCH=</b> exist(\$status)	<b>\$status</b> exists in the incoming event and is not an empty string.
isInt(String), isDouble (String)	Checks if the input string can be interpreted as an integer or a double number, respectively.	<b>\$MATCH=isDouble(\$size)</b>	the string value in \$size can be converted to a double.

Expressions and Functions	Description	Examples	True if
resolveHostIP (String host name)	Performs DNS resolution from a server to its IP address. If the DNS resolution fails, the function returns the value unknown host.	target_ip= resolveHostIP (\$host)	
resolveHostName (String host name)	Performs DNS resolution from an IP address to a fully qualified domain name. If the DNS resolution fails, the function returns the originally input host name.	target_name= resolveHostName (\$host)	

Any of the above expressions can be used and the expression can refer to incoming event fields. The value of the expression, which can be either **true** or **false**, determines whether the event handler is be used to process the event or not.

## Basic String Expressions

The following table summarizes the string expressions that can be used in the field mapping:

Operation	Description	Examples
+	String concatenation.	"trap type is " + \$trap
substring	Substring of given string.	\$var4.substring(3,5)
indexOf	Return indexOf string in another string.	\$var4.indexOf(\$var3)

## Basic Conditional Expression

One conditional expression is supported; the ? operator. This operator can be used to compose three expressions into one (for example, <Conditional part> ? <if true part> : <if false part>).

## Action Directive

The action directive has the form:

`$ACTION= TOPAZ_BUS_POST or DISCARD`

The value of the Action directive defines whether the event is processed and forwarded to Business Availability Center, or discarded. This value takes effect only if the matching condition within the handler had been evaluated to positive value (that is, to **true**). The table below describes the effect of the different actions.

Action	Description	For Use With
TOPAZ_BUS_POST (event)	Send the event to the Business Availability Center bus and database.	HP Business Availability Center
TOPAZ_BUS_POST (ss_t)	Send the metrics to HP Universal CMDB as SiteScope Data.	HP Business Availability Center
DISCARD	Do not send the data to HP Business Availability Center.	events you wish to filter out



---

**Note:** If you are using the metrics mapping, TOPAZ\_BUS\_POST(ss\_t), the data is sent to the HP Business Availability Center database as SiteScope data, and thus saved to the database. For details on metrics mapping, see “Configuring Field Mapping for Measurement Samples” on page 1156.

---

## Tags

In addition to directives, the event handler contains **tags**. Each tag represents a field in the event that is forwarded to Business Availability Center. The tag’s value can be evaluated when the event arrives to the integration monitor.

The general format of a tag is name[:type]=value.

The <name> is any string without spaces or dollar signs (\$). The <type> specifies the type of field as reported to Business Availability Center. It can be either **INT**, **DOUBLE** or **STRING**. The default type is **STRING**.

By defining a tag, you can customize event forwarding to Business Availability Center. Thus getting more value from the external applications that create those events. For example, if the monitor pulls out data from a database table column called `AlertText`, which contains a textual description of an alert, it is possible to send that data to Business Availability Center by adding the following line to an event handler section:

```
[event handler]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
text=$AlertText
```

---

**Note:** When adding tags, always add them after the **\$MATCH** and **\$ACTION**.

---

## Integration Monitor Field Mapping Examples

### Example 1: Universal Event Handler

```
[post them all]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL
szAlarmText:STRING="post them all handler received an event"
```

Note that the **\$MATCH** directive in the handler is set to **true**. This causes every event to match the handler and therefore every event is sent to the Business Availability Center bus.

### Example 2: Different Event Handlers for Different Severities

```
[Error Handler]
$MATCH= $status.equals("ERROR")
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_CRITICAL

[Info Handler]
$MATCH= $status.equals("INFO")
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL

[post them all]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL
```

In this example, an incoming event is matched against the **Error Handler** event handler. If the handler's condition is true (that is, the value in the status field equals **ERROR**), then an event with a field called severity, whose value is **SEVERITY\_CRITICAL**, is sent to HP Business Availability Center. An event can be matched only by a single handler. The first match stops the processing and therefore once an event is matched by a section, it is not processed by the next handler.

If the event was not matched by the first handler, the second handler comes into action and its match (which looks for status of **INFO**) is used to decide whether the second handler needs to take action. Finally, if the event does not match the second handler, the third universal handler is evaluated.



# 105

---

## HP OM Event Monitor

The HP OM Event Monitor allows you to integrate an existing Hewlett-Packard Operation Manager (OM) Server with HP Business Availability Center by transferring HP OM events from HP OM Server to an HP Business Availability Center server.

---

**Note:** This monitor supports:

- ▶ HP OM/UNIX versions 8.x (x >= 24) when installed on Solaris or on HP UX platforms.
  - ▶ HP OM/Windows versions 7.5x when installed on Windows platforms.
  - ▶ English only. It does not support I18N mode.
- 

### **This chapter includes:**

#### Concepts

- ▶ HP OM Event Monitor Overview on page 1174

#### Tasks

- ▶ HP OM Integration Add-on – Workflow on page 1175

#### Reference

- ▶ HP OM Event Monitor User Interface on page 1183

## HP OM Event Monitor Overview

The HP OM Event Monitor depends on an HP OM Integration Add-on module to collect events from the HP OM Server. The Add-on, when installed on the HP OM Server, listens to events received by the HP OM system and sends them to the HP OM Event Monitor. The HP OM Event Monitor transfers the events to an HP Business Availability Center server. The HP OM Integration Add-on and the HP OM Event Monitor communicate using TCP/IP networking (with a customizable TCP port).

The HP OM Event monitor uses a predefined configuration file, `<SiteScope root directory>\conf\ems\hp\event.config`, to define the processing of incoming data and to define the output sample forwarded to HP Business Availability Center. Do not modify this configuration file.

This section also includes:

- “Status” on page 1174
- “Configuring the Monitor” on page 1175

### Status

The status returned by the monitor is the current value of the monitor, such as:

```
Status: GOOD
Status Summary: 10 events received, connected Add-ons: 1
```

The status is logged as either good, warning, or error. A warning status is returned if no Add-on is connected to the monitor.

The status can be configured further using advanced options in the HP OM Alert Monitor Configuration Form.

For information about Integration Monitor logging and troubleshooting, see “Integration Monitor Logs” on page 1143 and “Troubleshooting and Limitations” on page 1143.

## Configuring the Monitor

For task details, see “HP OM Integration Add-on – Workflow” on page 1175.

For user interface details, see “HP OM Event Monitor User Interface” on page 1183.

### HP OM Integration Add-on – Workflow

The purpose of the HP OM Integration Add-on is to connect to the HP OM message infrastructure, to receive events from the HP OM, and to forward these events to the SiteScope machine.

---

**Note:** The HP OM Integration Add-on module is platform specific. Modules are provided for all platforms supported by OM/UNIX version 8.24 or OM/Windows version 7.5.

---

This task includes the following steps:

- “Install the HP OM Integration Add-on” on page 1176
- “Configure the HP OM Integration Add-on” on page 1177
- “Tune the HP OM Integration Add-on” on page 1178
- “Start and Stop the HP OM Integration Add-on” on page 1180
- “Uninstall the HP OM Integration Add-on files from the HP OM Server” on page 1181
- “Support in HP OM Cluster Installation” on page 1182
- “View Log File Messages” on page 1182

## 1 Install the HP OM Integration Add-on

Installation packages for the various platforms used below is in <SiteScope root directory>\conf\ems\hp\addon\OVO-BAC.zip file.

### To install on HP-UX 11.11:

- a** Log in as superuser to the HP OM Server. Alternatively, use the `su` command to gain superuser permissions.
- b** Copy `HPOvOBac-01.00.000-HPUX11.0-release.depot` installation package to `\tmp`.
- c** Perform the following command:  

```
swinstall -s /tmp/HPOvOBac-01.00.000-HPUX11.0-release.depot \*
```

### To install on HP-UX 11.23:

- a** Log in as superuser to the HP OM Server. Alternatively, use the `su` command to gain superuser permissions.
- b** Copy `HPOvOBac-01.00.000-HPUX11.22_IPF32-release.depot` installation package to `\tmp`.
- c** Perform the following command:  

```
swinstall -s /tmp/HPOvOBac-01.00.000-HPUX11.22_IPF32-release.depot \*
```

### To install on Solaris 5.7 or later:

- a** Log in as user root to the HP OM Server. Alternatively, use the `su` command to gain super-user permissions.
- b** Copy `HPOvOBac-01.00.000-SunOS5.7-release.sparc` installation package to `\tmp`.
- c** Perform the following command:  

```
pkgadd -d /tmp/HPOvOBac-01.00.000-SunOS5.7-release.sparc HPOvOBac
```



**To install on Windows:**

- a** Log in as user administrator to the HP OM Server.
- b** Copy **HPOvXpl-02.61.120-WinNT4.0-release.msi** and **HPOvOBac-01.00.000-WinNT4.0-release.msi** installation packages to **C:\tmp**. Perform the following commands:
  - `msiexec /I C:\tmp\HPOvXpl-02.61.120-WinNT4.0-release.msi /qn`
  - `msiexec /I C:\tmp\HPOvOBac-01.00.000-WinNT4.0-release.msi /qn`

**2 Configure the HP OM Integration Add-on**

Once installed, the HP OM Integration Add-on must be configured on the HP OM Server before it can be used.

**To configure the HP OM Integration Add-on on the HP OM Server:**

- a** Configure the host name or IP address of the SiteScope machine on which the HP OM Event Monitor is installed:  
`ovconfchg -ns opc.bac -set TargetHost <host name>`
- b** Configure the port if you are using a port other than the default (9000):  
`ovconfchg -ns opc.bac -set TargetHost <host name> -set TargetPort <port>`

---

**Note:** If you change this setting, make sure to update the HP OM Event Monitor.

---

HP OM Integration Add-on for UNIX provides a function that improves performance of internal message processing. Enabling this function improves the performance of the HP OM Integration Add-on (and other OM components, such as the OM Java GUI). This function is disabled by default.

**To enable improved HP-OM Add-on performance on UNIX feature:**

On the HP OM Server, perform the following commands:

- a** `opcsv -stop`
- b** `ovconfchg -ovrg server -ns opc -set OPCMSGM_USE_GUI_THREAD NO_RPC`
- c** `opcsv -start`

**3 Tune the HP OM Integration Add-on**

You can tune the HP OM Integration Add-on by running utilities from the command line on the HP OM Server.

**To check the current settings:**

Perform the following command:

`ovconfget opc.bac`

**To change a parameter:**

Perform the following command:

`ovconfchg -ns opc.bac -set <variable name> <value>`

where <variable name> and <value> are in the following table:

Variable Name	Default Value	Description
TargetHost	<empty>	Host name of the SiteScope receiver. No connection is attempted if this is empty.
TargetPort	9000	Port number of the SiteScope receiver. No connection is attempted if this is 0.
CacheMax	1000	Maximum number of messages stored in cache memory to avoid database lookups.
CacheKeep	500	If cache size reaches CacheMax, only the most-recently-used messages in CacheKeep are kept in the cache. All others are removed from the cache.

Variable Name	Default Value	Description
Connection Timeout	300	If no new messages or message changes are transmitted to the SiteScope receiver, the connection is closed after this number of seconds.
MinWaitTime	15	If the connecting to the SiteScope receiver failed, the HP OM Integration Add-on waits this many seconds the first time after connection failure before retrying to connect. The wait time is doubled after each retry, up to MaxWaitTime.
MaxWaitTime	120	Maximum number of seconds to wait after connection failures before retry. When doubling the wait time after connection failures exceeds MaxWaitTime, the wait time is no longer doubled and MaxWaitTime is used instead.
MaxQueueLen	1000	If the connection to the SiteScope receiver has been lost and new messages or message changes come in, these messages and message changes are buffered in a memory queue. If the number of entries in that queue reaches MaxQueueLen, the oldest entries are removed from the queue.
NodeKeepTime	900	The HP OM Integration Add-on looks up IP addresses from host names. In addition, OM/Windows host names also need to be looked up from the OM database. These IP addresses (and host names on OM/Windows) are stored in a memory cache. Because host names and IP addresses of systems can be changed, entries in that cache are invalidated (and afterwards looked up again) after NodeKeepTime seconds.

Changing any of these variables automatically updates the HP OM Integration Add-on. There is no need to stop and restart the HP OM Integration Add-on process.

## 4 Start and Stop the HP OM Integration Add-on

The HP OM Integration Add-on must be started after it is installed.

### To start and stop the HP OM Integration Add-on on UNIX platforms:

On UNIX platforms, the HP OM Integration Add-on is controlled by OpenView Control Daemon (ovcd). Using the command line tool **ovc** on the HP OM Server, perform the command:

```
ovc -stop <or start> opc2bac
```

If the HP OM Integration Add-on disconnects from SiteScope during operation, it tries to reconnect to the SiteScope at regular intervals. In the meantime, events are stored within the HP OM Integration Add-on.

If the HP OM Integration Add-on terminates from SiteScope during operation, the events not yet sent to SiteScope are lost.

---

**Note:** Because the Integration Add-on is linked with HP OM API libraries, it may be necessary to stop the Integration Add-on before installing HP OM patches, and start it after the patch installation.

---

### To start or stop the HP OM Integration Add-on on Windows platforms:

On Windows platforms, the HP OM Integration Add-on runs as a Windows service.

- a** On the HP OM Server, click **Start > Settings > Control Panel > Administrative Tools > Services**.
- b** Select the service **HP OpenView Operations Message Forwarder to BAC**.
- c** Click **Start** or **Stop**.

## 5 Uninstall the HP OM Integration Add-on files from the HP OM Server

If you must uninstall the HP OM Integration Add-on files from the HP OM Server, perform the following procedure:

**To remove the HP OM Integration Add-on files from an HP OM Server on HP-UX platform:**

- a** Log in as superuser.
- b** Perform the command:  
`swremove HPOvOInt.HPOVOBAC`

**To remove the HP OM Integration Add-on files from an HP OM Server on Solaris platform:**

- a** Log in as superuser.
- b** Perform the command:  
`pkgrm HPOvOBac`

**To remove the HP OM Integration Add-on files from an HP OM Server on Windows platform:**

- a** On the HP OM Server, click **Start > Settings > Control Panel > Administrative Tools > Services**.
- b** Remove the following installed programs:
  - HP OpenView Operations, BAC Integration
  - HP OpenView Cross Platform Components (unless used by other installed programs). If this program is in use, you receive an error message and the removal fails.

## 6 Support in HP OM Cluster Installation

The HP OM Integration Add-on is supported in an HP OM cluster environment. You can do the following tasks:

- Install HP OM Integration Add-on on each cluster node separately.
- Configure HP OM Integration Add-on on each cluster node separately. All configuration settings on all cluster nodes must be identical.
- Uninstall HP OM Integration Add-on on each cluster node separately.

## 7 View Log File Messages

On UNIX platforms, the HP OM Integration Add-on writes log messages into the log file `/var/opt/OV/logSystem.txt`.

On Windows platforms, `System.txt` is in directory `<DataDir>\log` where `<DataDir>` is the data directory chosen during OM/Windows installation (for example, `C:\Program Files\HP OpenView\Data`).

Log file entries use the process name `opc2bac` for messages logged by the HP OM Integration Add-on.

## HP OM Event Monitor User Interface

<p><b>Description</b></p>	<p>The HP OM Event Monitor allows you to integrate an existing HP OpenView installation with HP Business Availability Center by transferring HP OM messages from HP OM Server to an HP Business Availability Center server.</p> <p>This monitor supports:</p> <ul style="list-style-type: none"> <li>➤ HP OM versions 8.24 or later, when installed on Solaris 5.7 and later or when installed on HP UX 11.11 or HP UX 11.23</li> <li>➤ HP OM versions 7.5 or later when installed on Windows</li> </ul> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>➤ “HP OM Integration Add-on – Workflow” on page 1175</li> <li>➤ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ “HP OM Event Monitor” on page 1173</li> <li>➤ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## HP OM Event Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>HP OM Add-on TCP port</b>	Enter the TCP port number as configured in the HP OM Integration Add-on. <b>Default value:</b> 9000

## Field Mapping

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Field mapping</b>	<p>The out-of-the-box integration script that enables the monitor to correctly map the data it collects from the OM installation to a format recognizable by the monitor and HP Business Availability Center.</p> <p>We recommend that you use the field mapping as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the file in the following location and edit it in your preferred text editor: &lt;SiteScope root directory&gt;\conf\ems\hp\event.config. To enable any changes, you must edit the monitor to reload the edited script.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1147.</p>



## Topology Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Script</b>	<p>The out-of-the-box integration script that creates a topology in Business Availability Center that is based on the data collected from the OM installation. The script is based on the Jython scripting language (Python enabled by Java) and enables the integration between the data the monitor collects from the OM system and Business Availability Center's applications.</p> <p>We recommend that you use the topology settings as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the following file: &lt;SiteScope root directory&gt;\discovery\scripts\ems_hpovo.py and edit it in your preferred text editor. To enable any changes, you must edit the monitor to reload the edited script.</p> <p>For more details on editing the script, see "Topology Settings for Technology Integration Monitors" on page 1133.</p>



# 106

---

## HP Service Manager Monitor

The HP Service Manager Monitor enables you to integrate Incident Management data from an HP ServiceCenter or HP Service Manager installation with HP Business Availability Center. In general, this chapter uses the name Service Manager when referring to both ServiceCenter and Service Manager. If there are specific differences, they are noted.

---

### Note:

- ▶ This monitor supports ServiceCenter 6.2.6 and Service Manager 7.01, 7.02, and 7.1. Check the readme file for updates to the support matrix.
- ▶ SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various services and aspects of a Service Manager environment. For details, see “HP Service Manager Solution Template” on page 1703.

---

### This chapter includes:

#### Concepts

- ▶ HP Service Manager Monitor Overview on page 1188

#### Tasks

- ▶ HP Service Manager Integration – Workflow on page 1189

#### Reference

- ▶ HP Service Manager Monitor User Interface on page 1192

## **HP Service Manager Monitor Overview**

Use the HP Service Manager monitor in SiteScope to integrate the incident data from HP Service Manager to HP Business Availability Center.

Incident Management automates reporting and tracking an incident, or groups of incidents, associated with a business enterprise. Incident Management enables you to identify types of incidents, such as software, equipment, facilities, network, and so on, and track the resolution process of these incidents.

The HP Service Manager monitor forwards business service-related incidents to HP Business Availability Center to create configuration items (CIs) based on those incidents. By default, CIs are created only for those incidents that are considered business service incidents in HP Service Manager. If necessary for your environment, you can configure the integration scripts to map other incidents as well.

The integration maps the incidents to the business service CIs created and creates a monitored by relationship between the HP Service Manager monitor CI and the business service CI. The monitor integrates the incident data into samples which are forwarded to HP Business Availability Center applications, such as Dashboard and Service Level Management.

For more details on the capabilities of the integration, see “Introduction to HP Service Manager Integration” on page 3 in the HP Business Availability Center Documentation Library.

For more detailed information on the CIs and related KPIs, see “Integration with HP Service Manager” in *Using Service Level Management* in the HP Business Availability Center Documentation Library.

### **Configuring the Monitor**

For task details, see “HP Service Manager Integration – Workflow” on page 1189.

For user interface details, see “HP Service Manager Monitor User Interface” on page 1192.

## HP Service Manager Integration – Workflow

The following are the steps necessary to configure the integration:

- “Edit Clocks and Incident Management Configuration Files” on page 1189
- “Add or Create the JAR File (If Required)” on page 1189
- “Configure an HP Service Manager Monitor in SiteScope” on page 1190

### 1 Edit Clocks and Incident Management Configuration Files

If any changes were made to the clocks table and/or the incident management tables in HP Service Manager, then the same changes must be made to the corresponding configuration files in SiteScope. The configuration files included with the integration are configured with the same parameters as the default tables in HP Service Manager. However, if these tables were changed in any way, they must be edited on the SiteScope side as follows:

- a Access the files from the following location:
  - <SiteScope root directory>\conf\ems\peregrine\incidentAttributesMapping.config
  - <SiteScope root directory>\conf\ems\peregrine\clockAttributesMapping.config
- b Edit the files using a text editor. Follow the mapping directions as documented in the files.

### 2 Add or Create the JAR File (If Required)

You can add or create the JAR file for this monitor as follows:

- For integrations with ServiceCenter 6.2.6 and HP Service Manager 7.0.x using default settings, no additional JAR configurations are required.
- For integrations with HP Service Manager 7.1 using default settings, you must copy the JAR file to the **WEB-INF\lib** directory and edit the configuration file. For details, see “Copy the JAR File” on page 1190.

- ▶ For any integration with ServiceCenter or HP Service Manager that does not use the default configuration, you must create the JAR file. For details, see “Create the JAR File” on page 1191.

---

**Note:** SiteScope cannot monitor HP Service Manager 7.1 and earlier versions of HP Service Manager at the same time, since they require different JARs and configurations.

---

### 3 Configure an HP Service Manager Monitor in SiteScope

You can create this monitor:

- ▶ Using the EMS Integrations Administration portal in HP Business Availability Center
- ▶ Directly in SiteScope

For details on the user interface, see “HP Service Manager Monitor User Interface” on page 1192.

#### Copy the JAR File

To enable SiteScope to integrate with HP Service Manager 7.1 using default settings, copy the JAR file from **<SiteScope root directory>\conf\ems\peregrine\lib\7.1x** to **<SiteScope root directory>WEB-INF\lib**.

Open the **incidentAttributesMapping.config** file located in **<SiteScope root directory>conf\ems\peregrine**, and change the line **target\_name=configurationItem** to **target\_name=affectedItem**.

---

**Note:** The **peregrine.jar** located in **<SiteScope root directory>conf\ems\peregrine\lib\6x-7.0x** can be used as backup for the out-of-the-box JAR.

---

## Create the JAR File

This batch file creates and compiles the files needed for the HP Service Manager monitor. The result of this batch is the file **peregrine.jar** that is automatically copied to the **WEB-INF\lib** directory. You should also create a backup of the .jar file. To create the .jar file:

- 1 Stop the SiteScope service on the SiteScope machine.
- 2 Ensure that JDK version 1.5 is installed (1.5.0\_08 recommended -- can be downloaded from Sun archives, <http://java.sun.com/products/archive/>).
- 3 Set **JAVA\_HOME** system variable to the JDK directory (for example **C:\j2sdk1.5.0\_08**). You must recompile the peregrine.jar file if you made changes to the monitor tables.
- 4 Update the **<SiteScope root directory>\conf\ems\peregrine\build.properties** file with the wsdl locations.
  - When integrating with HP ServiceCenter 6.2.6, use the following syntax:  
 clocks.wsdl.url=http://<SM host>:<SM port>/sc61server/PW/Clocks?wsdl  
 prob.wsdl.url=http://<SM host>:<SM port>/sc61server/PW/IncidentManagement?wsdl
  - When integrating with Service Manager 7.x, use the following syntax:  
 clocks.wsdl.url=http://<SM host>:<SM port>/sc62server/PWS/Clocks?wsdl  
 prob.wsdl.url=http://<SM host>:<SM port>/sc62server/PWS/IncidentManagement?wsdl
- 5 Run the batch file:
  - **Windows:** Double-click the **<SiteScope root directory>\conf\ems\peregrine\create-peregrine-jar.bat** file to run the batch.
  - **UNIX:** You must run the **<SiteScope root directory>\conf\ems\peregrine\create-peregrine-jar.sh** file from the full path in a terminal window.
- 6 Restart the SiteScope service on the SiteScope machine.

## HP Service Manager Monitor User Interface

<p><b>Description</b></p>	<p>This monitor enables you to integrate HP Service Manager incidents with HP Business Availability Center. The incidents in Service Manager are forwarded to Business Availability Center as samples by this SiteScope monitor. The samples are used in reporting data to the Business Availability Center applications, such as Service Level Management and Dashboard.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<p>Monitors must be created in a group in the monitor tree. We recommend that you create a special group for the Service Manager integration.</p>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “HP Service Manager Integration – Workflow” on page 1189</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “HP Service Manager Monitor” on page 1187</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>



## HP Service Manager Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>HP Service Manager Web Service Endpoint</b>	<p>The URL for the HP Service Manager Web Service. Use the following format: <code>&lt;protocol&gt;://&lt;host_name&gt;:&lt;port&gt;/</code> where <b>host_name</b> is the name of the Service Manager server and <b>port</b> is the port number of the Service Manager server.</p> <p>The URL syntax when integrating with Service Manager 7.01 and 7.02 is: <code>&lt;protocol&gt;://&lt;SM host&gt;:&lt;SM port&gt;/sc62server/PWS/</code></p> <p>The URL syntax when integrating with Service Manager 6.2.6 is: <code>&lt;protocol&gt;://&lt;SM host&gt;:&lt;SM port&gt;/sc61server/ws</code></p>
<b>Username</b>	<p>The designated user name created in HP Service Manager for the purpose of this integration monitor.</p>
<b>Password</b>	<p>The password of the designated user created in HP Service Manager for the purpose of this integration monitor.</p>
<b>Field Mapping</b>	<p>The out-of-the-box integration script that enables the monitor to correctly map the data it collects from the Service Manager installation to a format recognizable by the monitor and HP Business Availability Center.</p> <p>We recommend that you use the field mapping as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the following file: <code>&lt;SiteScope root directory&gt;\conf\ems\peregrine\ticket.config</code> and edit it in your preferred text editor. To enable any changes, you must edit the monitor to reload the edited script.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1147.</p>

GUI Element	Description
<p><b>Test Script</b></p>	<p>Click to test the field mapping script. We recommend that you test the script before running the monitor. This test gives you the results of what events are forwarded to Business Availability Center. You can also view the results of the test in the following log file:  <b>&lt;SiteScope root directory&gt;\logs\bac_integration.log.</b></p> <p><b>Note:</b> The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>
<p><b>Synch Flag</b></p>	<p>Select to enable the monitor to query Service Manager to retrieve all Incidents Changes from the time specified in the <b>Synch Time</b> setting.</p> <p><b>Default value:</b> Cleared</p> <p><b>Note:</b> This flag is reset to cleared after each time the monitor retrieves the data from Service Manager.</p>
<p><b>Synch Time</b></p>	<p>Enter a value indicating the time from which the monitor retrieves incidents. Enter a value only when <b>Synch Flag</b> is selected.</p>

GUI Element	Description
<b>Incident Management (probsummary table) query</b>	<p>Enter the text to add to the query that the monitor sends to Service Manager. You can add to the query to determine which Incidents the monitor retrieves.</p> <p><b>Default value:</b> type="bizservice". The query is set to retrieve only those incidents opened on CIs of type <b>bizservice</b>.</p> <p><b>Note:</b> The syntax for the query must be specified by the Service Manager application. We recommend that you consult the Service Manager help to create the text to add to the query and to test the query using the advanced search found in the Service Manager application.</p>
<b>Incident Open State</b>	<p>Indicates the initial state as defined in Service Manager for the incident lifecycle.</p> <p><b>Default value:</b> Open</p>

## Topology Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<p><b>Script</b></p>	<p>The out-of-the-box integration script that creates a topology in Business Availability Center that is based on the data collected from the Service Manager installation. The script is based on the Jython scripting language (Python enabled by Java) and enables the integration between the data the monitor collects from the Service Manager system and Business Availability Center's applications.</p> <p>We recommend that you use the topology settings as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the following file: <b>&lt;SiteScope root directory&gt;\discovery\scripts\EMS_peregrine.py</b> and edit it in your preferred text editor. To enable any changes, you must edit the monitor for SiteScope to reload the edited script.</p> <p>For more details on editing the script, see "Topology Settings for Technology Integration Monitors" on page 1133.</p>
<p><b>Test Script</b></p>	<p>Click to test the topology script. This test gives you the results of what events are forwarded to Business Availability Center and what topology is mapped.</p> <p>You can also view the results of the test in the following log file: <b>&lt;SiteScope root directory&gt;\logs\bac_integration.log</b>.</p> <p><b>Note:</b> The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

# 107

---

## NetScout Event Monitor

The NetScout Event Monitor monitors alerts received from the NetScout nGenius server and forwards them to HP Business Availability Center. This provides a way to centralize data collection, display, and alerting for the conditions for which you may otherwise be unaware until something more serious happens.

### **This chapter includes:**

#### Concepts

- ▶ NetScout Event Monitor Overview on page 1198

#### Tasks

- ▶ NetScout Integration – Workflow on page 1200

#### Reference

- ▶ NetScout Event Monitor User Interface on page 1201

## NetScout Event Monitor Overview

The NetScout Event Monitor is designed to collect SNMP Trap data from NetScout nGenius servers. Each time that the monitor is run, SiteScope checks traps that have been received since the last time the monitor ran and reports the results to HP Business Availability Center.

The NetScout Event Monitor forwards alerting instances to HP Business Availability Center to create configuration items (CIs) based on application or host alarms in NetScout.

The integration maps the alarms to the NetScout CIs created and creates a monitored by relationship between the NetScout Event monitor CI and the relevant host, interface, or application CI. The monitor integrates the incident data into samples that are forwarded to HP Business Availability Center applications, such as Dashboard and Service Level Management.

---

**Note:** For information about Integration Monitor logging and troubleshooting, see “Integration Monitor Logs” on page 1143 and “Troubleshooting and Limitations” on page 1143.

---

This section also includes:

- ▶ “Setup Requirements” on page 1199
- ▶ “Configuring the Monitor” on page 1199

## Setup Requirements

The following are important guidelines and requirements for using the NetScout Event Monitor to forward alerts to HP Business Availability Center.

- ▶ The NetScout nGenius server must be configured to send traps to the SiteScope server.

---

**Note:** The NetScout Event Monitor uses port 162 for receiving traps. If another application or process on the machine where SiteScope is running has bound this port, the monitor reports an **Address in use** error and the monitor type is unavailable.

---

- ▶ SiteScope must be registered with an HP Business Availability Center installation. The SiteScope must have a profile defined in the HP Business Availability Center installation prior to enabling the registration in the SiteScope interface. To verify registration or to re-register SiteScope with HP Business Availability Center, see the Integration Preferences page in the Preferences container.
- ▶ The NetScout Event Monitor must be set to synchronize integration monitor data with HP Business Availability Center. You can use the configuration file for the NetScout Event Monitor to control the data that is sent from SiteScope to HP Business Availability Center. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 1147.

## Configuring the Monitor

For task details, see “NetScout Integration – Workflow” on page 1200.

For user interface details, see “NetScout Event Monitor User Interface” on page 1201.

## **NetScout Integration – Workflow**

The following are the tasks necessary to integrate data from a NetScout system and view the NetScout data in a way that is customized to your needs.

This task includes the following steps:

- “Configure a NetScout Event Monitor in SiteScope” on page 1200
- “Activate NetScout EMS Integration in Business Availability Center” on page 1200

### **1 Configure a NetScout Event Monitor in SiteScope**

You can create this monitor:

- Directly in SiteScope
- Using the System Availability Management Administration portal in HP Business Availability Center

For details on the monitor’s settings, see “NetScout Event Monitor User Interface” on page 1201.

### **2 Activate NetScout EMS Integration in Business Availability Center**

Activate the assignment rules in Business Availability Center. For details on how to perform this task, see “NetScout nGenius Integration” in *Solutions and Integrations* in the HP Business Availability Center Documentation Library.



## NetScout Event Monitor User Interface

<b>Description</b>	<p>The NetScout Event Monitor monitors alerts received from the NetScout nGenius server and forwards them to HP Business Availability Center.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	Monitors must be created in a group in the monitor tree.
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “NetScout Integration – Workflow” on page 1200</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “NetScout Event Monitor” on page 1197</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## NetScout Event Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Run Alerts</b>	<p>Select the method for running alerts:</p> <ul style="list-style-type: none"> <li>➤ If <b>for each event received from NetScout system</b> is chosen, then the monitor triggers alerts for every matching entry found.           <p><b>Note:</b> If <b>for each event received from NetScout system</b> is selected as the alert method, when the NetScout Monitor is run, the monitor never reports a status of error or warning, regardless of the results of the content match or even if the target SNMP Trap is not found.</p> </li> <li>➤ If the <b>once, after all events from NetScout system were received</b> method is selected, then the monitor counts up the number of matches and triggers alerts based on the <b>Error if</b> and <b>Warning if</b> thresholds defined for the monitor in the Threshold Setting section.</li> </ul>
<b>EMS Time Difference</b>	<p>Enter a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded.</p> <p><b>Note:</b> The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.</p>

## Field Mapping

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Field Mapping</b>	<p>The out-of-the-box integration script that enables the monitor to correctly map the data it collects from the NetScout installation to a format recognizable by the monitor and HP Business Availability Center.</p> <p>This script is not editable.</p>

## Topology Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Script</b>	<p>The out-of-the-box integration script that creates a topology in Business Availability Center. The topology is based on the data collected from the NetScout installation. The script is based on the Jython scripting language (Python enabled by Java) and enables the integration between the data the monitor collects from the NetScout system and Business Availability Center's applications.</p> <p>We recommend that you use the topology settings as is and it is not editable while creating the monitor. If you must customize the topology, locate the following file:  <b>&lt;SiteScope root directory&gt;\discovery\scripts\ems\ems_netscout.py</b>  and edit it in your preferred text editor. To enable any changes, you must edit the monitor to reload the edited script.</p> <p>For more details on editing the script, see "Topology Settings for Technology Integration Monitors" on page 1133.</p>



## Technology Database Integration Monitor

The Technology Database Integration Monitor allows you to collect event and time series data from database tables used by Enterprise Management Systems (EMS) by performing a query through a JDBC connection. The data retrieved is then processed and sent to HP Business Availability Center as samples (one sample for each row that was returned by a SQL query).

### **This chapter includes:**

#### Concepts

- ▶ Technology Database Integration Monitor Overview on page 1206

#### Tasks

- ▶ Integrate Database Data into HP Business Availability Center on page 1210

#### Reference

- ▶ Technology Database Integration Monitor User Interface on page 1214
- ▶ Troubleshooting and Limitations on page 1223

## Technology Database Integration Monitor Overview

Use the Technology Database Integration Monitor to integrate database records into HP Business Availability Center. The following are examples of data that can be integrated into HP Business Availability Center using the Technology Database Integration Monitor:

- ▶ Events from monitoring applications event tables or views.
- ▶ Open tickets from ticketing systems applications.
- ▶ Time series from monitoring applications measurement tables.

Each time the Technology Database Integration Monitor runs, it returns the monitors status, the time it took to perform the query, the number of rows in the query result set, and the first two fields in the first row of the result and writes them in the monitoring log file.

This section includes the following topics:

- ▶ “What Data Is Forwarded” on page 1206
- ▶ “Setup Requirements” on page 1207
- ▶ “Notes and Limitations” on page 1209
- ▶ “Configuring the Monitor” on page 1209

### What Data Is Forwarded

The Technology Database Integration Monitor uses a user-defined query and enumerating field name, field type, and initial value. While the query provided by the user is used to define a search criterion on the database, the enumerating field is used so that events are forwarded only once. Using an initial value allows you to specify an initial threshold value for the events that should be forwarded.

For example, if **Enumerating Field Type** uses DATE and **Start from value** uses 2003-20-03 12:00:00, only events that happened after the specified date are forwarded in the first run of the monitor. In subsequent monitor runs, the highest value for the DATE field found is used to verify that only new events are forwarded.

You use the field mapping script selected for the Technology Database Integration Monitor to control the data that is sent from SiteScope to Business Availability Center. See the section on “Integration Monitor Field Mapping” on page 1147 for more details on the file structure and syntax.

Before setting up the Technology Database Integration Monitor, you should be clear about the purpose and usage of the data in HP Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

## Setup Requirements

The steps for setting up a Technology Database Integration Monitor vary according to what database software you are trying to query. The following is an overview of the requirements for using the Technology Database Integration Monitor:

- ▶ You must use one of the database drivers supplied by default, or install or copy a compatible database driver or database access API into the required SiteScope directory location. The supplied drivers include:
  - ▶ **com.inet.tds.TdsDriver.** TDS driver is from i-net Software for Microsoft SQL databases. This driver is deployed with SiteScope.
  - ▶ **com.mercury.jdbc.sqlserver.SQLServerDriver.** DataDirect driver is from DataDirect Technologies. It is an alternative to the TDS driver for those Microsoft SQL databases that use Windows NT authentication. This driver is deployed with SiteScope.
  - ▶ **com.inet.ora.OraDriver.** OraDriver driver is from Oracle for Oracle databases. This driver is deployed with SiteScope.

Other database driver packages are available as compressed (zipped) archive files or .jar files. Database drivers in this form must not be extracted. Rather, put them into the **<SiteScope root directory>\java\lib\ext** subdirectory.

- ▶ You must know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers.

Database Connection URLs for this monitor are:

- ▶ **`jdbc:inetdae:<hostname>:<port>`**  
where `<hostname>` is the name of the host where the database is running and `<port>` is the port on which the database interfaces with the driver.
- ▶ **`jdbc:mercury:sqlserver://<hosthost>:1433;DatabaseName=master;AuthenticationMethod=type2`**  
where `<hostname>` is the name of the host where the database is running.
- ▶ **`jdbc:oracle:thin:@<hostname>:<port>:<dbname>`**  
**where `<hostname>` is the name of the host where the database is running, `<port>` is the port on which the database interfaces with the driver, and `<dbname>` is the name of the Oracle database instance.**
- ▶ The database you want to query must be running, have a database name defined, and have at least one named table created in the database. In some cases, the database management software needs to be configured to enable connections by using the middleware or database driver.
- ▶ You need a valid user name and password to access and perform a query on the database. In some cases, the machine and user account that SiteScope is running on must be given permissions to access the database.
- ▶ You must know a valid SQL query string for the database instance and database tables in the database you want to query. Consult your database administrator to work out required queries to use.
- ▶ When adding the monitor to SiteScope, in the Field Mapping panel, you must select a field mapping script and load the script for the monitor. Copy the contents of the script into your preferred text editor, and edit the script to define the event handlers for this monitor instance. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 1147.



## Notes and Limitations

- ▶ When Windows authentication is used to connect to the database, configure SiteScope using the following settings:
  - ▶ JDBC Connection string: **jdbc:mercury:sqlserver://<hosthost>:1433; DatabaseName=master;AuthenticationMethod=type2**
  - ▶ JDBC driver: **com.mercury.jdbc.sqlserver.SQLServerDriver**.
  - ▶ Leave the **Database User name** and **Database Password** fields empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.
- ▶ When referring to data arriving from the Technology Database Integration Monitor in the config file, use the column name prefixed by the dollar sign (\$).

For example, for the following database query:

```
SELECT height,width FROM some_table WHERE width > 0
```

You can refer to the columns returned using the labels \$height and \$width. The names of the columns are case sensitive.

## Configuring the Monitor

For task details, see “Integrate Database Data into HP Business Availability Center” on page 1210.

For user interface details, see “Technology Database Integration Monitor User Interface” on page 1214.

## **Integrate Database Data into HP Business Availability Center**

This section provides the workflow for setting up the Technology Database Integration Monitor to work with HP Business Availability Center. If you need more information on performing any of the steps, see the sections on “Setup Requirements” on page 1207, and “Technology Database Integration Monitor User Interface” on page 1214.

This task includes the following steps:

- “Prerequisites” on page 1211
- “Use the SiteScope Database Connection Tool” on page 1211
- “Create a Technology Database Integration Monitor” on page 1212
- “Edit the Monitor’s Field Mappings” on page 1212
- “Edit the Monitor’s Topology Settings - Optional” on page 1213
- “View Data from the Monitor in HP Business Availability Center” on page 1213

## 1 Prerequisites

- a** Use a database client to connect to the relevant software database. Identify which tables contain the required events/metrics (the software schema documentation may help you with this).
- b** A JDBC database driver is a prerequisite for setting up the monitor. We recommend that you use the following JDBC drivers:

- For SQL Server:

**Database Connection URL=**  
**jdbc:inetdae:<DatabaseHostName>:<Port>?database=<Database Name>**

**Database Driver=com.inet.tds.TdsDriver**

- For Oracle:

**Database Connection URL=**  
**jdbc:inetora:<DatabaseHostName>:<Port>:<Database Instance Name>**

**Database Driver=com.inet.ora.OraDriver**

## 2 Use the SiteScope Database Connection Tool

Run the SiteScope Database Connection tool and follow these steps:

- a** Verify the driver can be loaded and that it successfully connects.
- b** Add a user name and password to verify that a connection can be established to the database.
- c** Add a native query. Refine the query until you get all the required events/metrics required for HP Business Availability Center.

### 3 Create a Technology Database Integration Monitor

Add a Technology Database Integration Monitor to SiteScope. For details on the user interface, see “Technology Database Integration Monitor User Interface” on page 1214.

- When adding the new monitor to a group, it is recommended that you use a dedicated group for integration monitors only.
- If you do not see the **Integration Monitors** category, make sure you have an EMS Option License for your SiteScope.
- **Name.** It is recommended that the monitor name include the name of the integrated software.
- Enter all connection parameters for connecting to the database in the **Connection parameters** area.
- **SELECT/FROM/WHERE query clauses.** **SELECT** and **FROM** are mandatory. When specifying the **SELECT** clause, the value given for **Enumerating field** must appear in the clause.
- **Frequency.** Define how often the monitor should query the database. The maximum number of rows that the monitor can retrieve on each cycle is 5000; this is to prevent an out-of-memory exception. The frequency should therefore be set so that the monitor retrieves a maximum of 5000 rows per cycle.

You can edit the maximum number of rows in the **Query Settings** section for the monitor.

- **Enumerating field parameters.** Enter details for the enumerating field.

### 4 Edit the Monitor’s Field Mappings

In the New Technology Database Integration Monitor dialog box, expand the Field Mapping area. Select a field mapping type and click **Load Script**.

- If you select **Events** or **Metrics**, a template script is displayed in the **Field mapping** box. Edit the script to enable SiteScope to retrieve the data from the monitored application that you want to forward to Business Availability Center.

- If you select **Custom**, create your own script to map the fields for retrieving data from the monitored application.

For details on working with the field mapping script, see “Integration Monitor Field Mapping” on page 1147.

For details on the user interface, see “Field Mapping” on page 1219.

## 5 Edit the Monitor’s Topology Settings - Optional

Optionally, in the New Technology Database Integration Monitor dialog box in the Topology Settings area, you can create a Jython script that creates a topology of configuration items in HP Business Availability Center’s CMDB to match your EMS system. You copy the script into the Script field in the Topology Settings.

For details on this topic, see “Topology Settings for Technology Integration Monitors” on page 1133.

For details on the user interface, see “Topology Settings” on page 1221.

## 6 View Data from the Monitor in HP Business Availability Center

View the data in HP Business Availability Center:

- **Events integration.** If you chose and edited the Events script in the Field Mapping area, you can view events in Dashboard, System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- **Metrics integration.** If you chose and edited the Metrics script in the Field Mapping area, you can view the data in any application that supports SiteScope data, including SiteScope Over Time reports.
- If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <HP Business Availability Center root directory>\bin.

To troubleshoot problems with data arriving to HP Business Availability Center, see “Troubleshooting and Limitations” on page 1223.

 **Technology Database Integration Monitor User Interface**

<b>Description</b>	<p>The Technology Database Integration Monitor allows you to collect event and time series data from database tables used by Enterprise Management Systems (EMS) by performing a query through a JDBC connection. The data retrieved is then processed and sent to HP Business Availability Center as samples (one sample for each row that was returned by a SQL query).</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>Database Connection Tool</b> is available when configuring this monitor to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “Database Connection Tool” on page 198.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Integrate Database Data into HP Business Availability Center” on page 1210</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Technology Database Integration Monitor” on page 1205</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Technology Database Integration Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Basic Settings</b>	
<b>Database connection URL</b>	<p>Enter a URL to a database connection (sometimes referred to as an Authentication string).</p> <p>One way to create a database connection is to use ODBC to create a named connection to a database. For example, first use the ODBC control panel to create a Data Source Name (DSN) called <code>test</code> under the system DSN tab. Then, enter <code>jdbc:odbc:test</code> as the connection URL. Alternatively, use the supplied Microsoft SQL or Oracle driver to connect to the Database.</p>
<b>Database driver</b>	Enter the driver used to connect to the database. Use the Fully Qualified Class Name of the JDBC driver you are using.
<b>Database user name</b>	Enter the user name used to login to the database.
<b>Database password</b>	Enter a password used to login to the database.
<b>OS integrated security</b>	<p>Check this check box if you want to use the user name and password from Windows' user authentication to access the database. Entries in the Database Username and Database Password are ignored.</p> <p>If this parameter is checked, you must use the DataDirect driver as your database driver.</p>

GUI Element	Description
<b>EMS server name</b>	<p>If you are reporting monitor data to an installation of HP Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in an HP Business Availability Center report.</p> <p><b>Syntax exceptions:</b> Use only alphanumeric characters for this entry. You can enter the name of the monitored server or a description of the database to be used to identify the host.</p>
<b>EMS time difference</b>	<p>Enter a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded.</p> <p>You can also view the results of the test in the following log file: <b>&lt;SiteScope root directory&gt;\logs\bac_integration.log</b>.</p> <p><b>Note:</b> The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.</p>
<b>Query Settings</b>	
<b>SELECT</b>	<p>Enter the SELECT clause to be used in the SQL query. Enter * for all fields or a comma separated list of column names to be retrieved from the database.</p> <p>When specifying the SELECT clause, the column used as the enumerating field must appear in the clause.</p>
<b>FROM</b>	<p>Enter the FROM clause to be used in the SQL query. Enter a table name or a comma separated list of tables from which the selected columns should be extracted.</p>



GUI Element	Description																				
<b>WHERE</b>	<p>Enter the WHERE clause to be used in the SQL query. This is an optional field which allows you to define the select criteria.</p> <p>Leaving it empty results in retrieving all the rows from the table defined in the FROM option.</p>																				
<b>Enumerating field</b>	<p>Enter a name for a database field that can be used to order the events that are returned from the database query.</p> <p><b>Note:</b> The column used as enumerating field must be included in the SELECT clause.</p>																				
<b>Enumerating field type</b>	<p>Enter the type of field used to order the result set. This can be a DATE field, an INTEGER field, a DOUBLE floating point numeral field, or a LONG field.</p> <p>The following table maps SQL types to the required enumerating field type.</p> <table border="1" data-bbox="621 789 1163 1206"> <thead> <tr> <th data-bbox="621 789 849 824">SQL Type</th> <th data-bbox="849 789 1163 824">Enumerating Field Type</th> </tr> </thead> <tbody> <tr> <td data-bbox="621 833 849 859">SMALLINT</td> <td data-bbox="849 833 1163 859">INTEGER</td> </tr> <tr> <td data-bbox="621 876 849 902">INTEGER</td> <td data-bbox="849 876 1163 902">INTEGER / LONG</td> </tr> <tr> <td data-bbox="621 920 849 946">BIGINT</td> <td data-bbox="849 920 1163 946">LONG</td> </tr> <tr> <td data-bbox="621 963 849 989">NUMERIC</td> <td data-bbox="849 963 1163 989">LONG</td> </tr> <tr> <td data-bbox="621 1006 849 1032">DOUBLE</td> <td data-bbox="849 1006 1163 1032">DOUBLE</td> </tr> <tr> <td data-bbox="621 1050 849 1076">DECIMAL</td> <td data-bbox="849 1050 1163 1076">DOUBLE</td> </tr> <tr> <td data-bbox="621 1093 849 1119">FLOAT</td> <td data-bbox="849 1093 1163 1119">DOUBLE</td> </tr> <tr> <td data-bbox="621 1137 849 1163">TIMESTAMP</td> <td data-bbox="849 1137 1163 1163">TIMESTAMP</td> </tr> <tr> <td data-bbox="621 1180 849 1206">DATE</td> <td data-bbox="849 1180 1163 1206">TIMESTAMP</td> </tr> </tbody> </table>	SQL Type	Enumerating Field Type	SMALLINT	INTEGER	INTEGER	INTEGER / LONG	BIGINT	LONG	NUMERIC	LONG	DOUBLE	DOUBLE	DECIMAL	DOUBLE	FLOAT	DOUBLE	TIMESTAMP	TIMESTAMP	DATE	TIMESTAMP
SQL Type	Enumerating Field Type																				
SMALLINT	INTEGER																				
INTEGER	INTEGER / LONG																				
BIGINT	LONG																				
NUMERIC	LONG																				
DOUBLE	DOUBLE																				
DECIMAL	DOUBLE																				
FLOAT	DOUBLE																				
TIMESTAMP	TIMESTAMP																				
DATE	TIMESTAMP																				

GUI Element	Description
<b>Initial enumerating value</b>	<p>Enter an initial value to be used as a condition for the initial run of this monitor instance. For example, if you specify the <b>Enumerating Field Type</b> as a field type DATE and you enter a value of 2000-01-31 12:00:00 in the <b>Start from</b> value field, only records that were added to the database after the specified date are forwarded.</p> <p><b>Note:</b> The value of this field cannot be edited.</p>
<b>Max rows</b>	<p>Specify the maximum number of rows the monitor retrieves from the database for each monitor cycle.</p> <p><b>Default value:</b> 5000 rows</p> <p>If the number of result rows exceeds the set maximum, the monitor retrieves the remaining rows (those that exceeded the maximum) on future cycles, until all result rows are retrieved.</p> <p>The value should be sufficient to keep up with database table growth, yet small enough to avoid <code>java.lang.OutOfMemoryException</code> errors. Further, monitor run frequency should also be considered. Make sure that the rate at which data is collected by the monitor—which is dependent on both monitor run frequency and network/system speed—is greater than, or equal to, the rate of data insertion on the monitored system.</p>

## Field Mapping

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Sample type</b>	Select from the following sample types for this integration: <ul style="list-style-type: none"> <li>▶ <b>Events.</b> For details, see “Configuring Field Mapping for Event Samples” on page 1150.</li> <li>▶ <b>Measurements.</b> For details, see “Configuring Field Mapping for Measurement Samples” on page 1156.</li> <li>▶ <b>Tickets.</b> For details, see “Configuring Field Mapping for Ticket Samples” on page 1159.</li> </ul>
<b>Load File</b>	Click to load the script that is applicable to the sample type selected above.
<b>Field mapping</b>	<p>The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring.</p> <p>The mapping is editable in this box. You can also copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1147.</p>

GUI Element	Description
<b>Test Script</b>	<p>Click to test the field mapping script. We recommend that you test the script before running the monitor. This test gives you the results in a separate window of what events or measurements are forwarded to Business Availability Center.</p> <p>You can also view the results of the test in the following log file: &lt;SiteScope root directory&gt;\logs\bac_integration.log.</p> <p><b>Note:</b> The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Topology Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Topology template</b>	<p>Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propagates its status to the CIs mapped in this topology.</p> <p>Select from:</p> <ul style="list-style-type: none"> <li>▶ <b>Custom.</b> You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the available topology.</li> <li>▶ <b>Hosts.</b> Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the topology.</li> <li>▶ <b>Hosts-Applications.</b> Creates a topology with an application CI and a host CI and an EMS monitor CI as the leaf node under each application CI and host CI.</li> </ul> <p><b>Note:</b> We recommend not to select <b>Custom</b> as this does not load a script and you must enter the entire script yourself. We recommend that you begin with either <b>Host</b> or <b>Host and Application</b> and edit one of those scripts. When editing the topology, you must make sure that an EMS Monitor CI is created as the leaf node to any CI that receives samples from the integration.</p> <p>For more details, see “Topology Settings for Technology Integration Monitors” on page 1133.</p>
<b>Load Script</b>	<p>Click to load the required Jython script for the topology you selected in the <b>Topology template</b> option. If you selected <b>Custom</b>, there is no script to load.</p>

GUI Element	Description
<p><b>Script</b></p>	<p>The contents of the script are editable in this box. However, it is recommended not to edit the contents of the script here. Copy the contents of the script into your preferred text editor, edit the script as needed, and then copy the contents back into this box.</p> <p><b>Note:</b> The Jython script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see “Topology Settings for Technology Integration Monitors” on page 1133.</p>
<p><b>Test Script</b></p>	<p>Click to test the topology script. We recommend that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is created. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: &lt;SiteScope root directory&gt;\logs\bac_integration.log.</p> <p><b>Note:</b> The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Troubleshooting and Limitations

- ▶ Check for errors in **<SiteScope root directory>\logs\RunMonitor.log** and in **<SiteScope root directory>\logs\error.log**.
- ▶ Change the log level to DEBUG in **<SiteScope root directory>\conf\core\Tools\log4j\PlanJava\log4j.properties**, to watch outgoing samples.

Change the line:

```
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
to:
```

```
log4j.category.EmsEventPrinter= DEBUG, ems.appender.
```

The log file to look at is:

**<SiteScope root directory>\logs\RunMonitor.log**

- ▶ If samples are created and sent from SiteScope, but the data is not seen in **Dashboard/Event Log/SiteScope reports**, look in **<HP Business Availability Center root directory>\log\mercury\_wde\wdeIgnoredSamples.log** to make sure the samples were not dropped due to missing fields or values.
- ▶ Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine:  
**<HP Business Availability Center root directory>\conf\core\tools\log4j\mercury\_wde\wde.properties**

Change the log level parameter to DEBUG in the following lines:

- ▶ `log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender`
- ▶ `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender`

Look at the corresponding log files:

- ▶ **<HP Business Availability Center root directory>\logs\mercury\_wde\wdeIgnoredSamples.log**
- ▶ **<HP Business Availability Center root directory>\logs\mercury\_wde\wdePublishedSamples.log**





# 109

---

## Technology Log File Integration Monitor

The Technology Log File Integration Monitor watches for specific entries added to a log file of an Enterprise Management System (EMS) application by trying to match against a regular expression. From each matched entry, one sample is created and sent to HP Business Availability Center. Each time the monitor runs, it examines log entries added since the last time it ran.

### **This chapter includes:**

#### Concepts

- ▶ Technology Log File Integration Monitor Overview on page 1226

#### Tasks

- ▶ Integrate Log File Data into HP Business Availability Center on page 1228

#### Reference

- ▶ Technology Log File Integration Monitor User Interface on page 1232

#### Troubleshooting and Limitations on page 1240

## Technology Log File Integration Monitor Overview

The Technology Log File Integration Monitor is useful for automatically extracting data from log files and sending the data to HP Business Availability Center.

Each time that SiteScope runs this monitor, the monitor starts from the point in the file where it stopped reading the last time the monitor ran. This insures that you are notified only of new entries and speeds the rate at which the monitor runs.

When using a regular expression to match against a specific line in the log, it is possible to use regular expression back references to select the data to be forwarded to Business Availability Center. For details on using back references, see “Retaining Content Match Values” on page 273.

This section includes the following topics:

- ▶ “What Data Is Collected” on page 1226
- ▶ “Setup Requirements” on page 1227
- ▶ “Configuring the Monitor” on page 1228

### **What Data Is Collected**

The Technology Log File Integration monitor sends to Business Availability Center data that is extracted from any row that matched against the **Content match** regular expression.

Before setting up the Technology Log File Integration Monitor, you should be clear about the purpose and usage of the data in HP Business Availability Center (for presentation in Dashboard, Service Level Management, and reports).

The specific data that is forwarded to HP Business Availability Center is controlled by the field mapping script. You use this script to specify the preferred value fields that you want forwarded. For more details on selecting the script and the file structure and syntax, see “Integration Monitor Field Mapping” on page 1147.

## Setup Requirements

The following are requirements for using the Technology Log File Integration Monitor to forward data to Business Availability Center:

- ▶ You must have the format and syntax of the log file that you want to monitor. You must construct a **Content match** regular expression to match on the entries in the log file that contain the data you want to monitor and forward to Business Availability Center. For examples of regular expressions, see “Examples for Log File Monitoring” on page 279.
- ▶ When adding the monitor to SiteScope, in the Field Mapping panel, you must select a field mapping script and load the script for the monitor. Edit the script to define the event handlers for this monitor instance. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 1147.

---

**Note:** When referring to data arriving from the Technology Log File Integration monitor in the configuration file, use the number corresponding to the back reference returned prefixed by the label `$group`.

For example, for the **Content Match** expression:

```
/([0-9]{2})\s([A-Z]*) ([a-z]*) /
```

and the corresponding Log file text that contains:

```
21 HELLO world
```

You can refer in the config file to three retained values (back references) as follows, where the number appended to the end of the `$groupn` label corresponds to the order of the parentheses in the expression:

```
$group0 = (21)
```

```
$group1 = (HELLO)
```

```
$group2 = (world)
```

---

## Configuring the Monitor

For task details, see “Integrate Log File Data into HP Business Availability Center” on page 1228.

For user interface details, see “Technology Log File Integration Monitor User Interface” on page 1232.

## Integrate Log File Data into HP Business Availability Center

This section provides the overall flow for setting up the Technology Log File Integration Monitor to work with HP Business Availability Center. If you need more information on performing any of the steps, see the sections on “Setup Requirements” on page 1227, or “Technology Log File Integration Monitor User Interface” on page 1232.

This task includes the following steps:

- ▶ “Analyze the Log File to Be Monitored” on page 1229
- ▶ “Create a Technology Log File Integration Monitor” on page 1229
- ▶ “Edit the Monitor’s Field Mapping” on page 1230
- ▶ “Edit the Monitor’s Topology Settings - Optional” on page 1230
- ▶ “Check the Regular Expression - Optional” on page 1230
- ▶ “View Data from the Monitor in HP Business Availability Center” on page 1231

## 1 Analyze the Log File to Be Monitored

Open the relevant software log file, and identify which lines describe events or measurements. Build your regular expression with the SiteScope Regular Expression tool. Use the tool to:

- Match against the line you wish to monitor.
- Make sure that values are extracted correctly from the line.

For details on the user interface, see “Regular Expression Tool” on page 232.

## 2 Create a Technology Log File Integration Monitor

Add a Technology Log File Integration Monitor to SiteScope. For details on the user interface, see “Technology Log File Integration Monitor User Interface” on page 1232.

- When adding the new monitor to a group, it is recommended that you use a dedicated group for integration monitors only.
- If you do not see the **Integration Monitors** category, make sure you have an EMS Option License for your SiteScope.
- **Name.** It is recommended that the monitor name include the name of the integrated software.
- **Log file path name and Server:**
  - The file name can include a variable name (for example: `s/c:\temp\EV-$year$-$0month$-$0day$.tab/`).
  - When reading a file on a remote UNIX machine, define a remote UNIX connection; you can then select the UNIX machine from the **Server** list.
  - When reading a file on a remote Windows machine, enter the UNC path in the **Log file path name** field (SiteScope should run under a privileged user for the machine that holds the file), and leave the **Server** box empty.
- **Content match (regular expression).** Surround values you wish to extract with parenthesis. It is recommended that you build your content match with the SiteScope Regular Expression tool before defining the monitor.

### 3 Edit the Monitor's Field Mapping

In the New Technology Log File Integration Monitor dialog box, expand the Field Mapping area. Select a field mapping type and click **Load Script**.

- ▶ If you select **Events**, **Tickets**, or **Measurements**, a template script is displayed in the **Field mapping** box. Edit the script to enable SiteScope to retrieve the data from the monitored application that you want to forward to Business Availability Center.
- ▶ If you select **Custom**, create your own script to map the fields for retrieving data from the monitored application.

For details on working with the field mapping script, see “Integration Monitor Field Mapping” on page 1147.

For details on the user interface, see “Field Mapping” on page 1236.

### 4 Edit the Monitor's Topology Settings - Optional

Optionally, in the New Technology Log File Integration Monitor dialog box in the Topology Settings area, you can create a Jython script that creates a topology of configuration items in HP Business Availability Center's CMDB to match your EMS system. You copy the script into the Script field in the Topology Settings.

For details on this topic, see “Topology Settings for Technology Integration Monitors” on page 1133.

For details on the user interface, see “Topology Settings” on page 1238.

### 5 Check the Regular Expression - Optional

After entering the settings for the Technology Log File Integration Monitor, it is recommended that you perform optimization of the regular expression (for example, to check for problems with use of quantifiers such as `.*`). Use the SiteScope Regular Expression tool to perform the optimization. Update the monitor with any corrections.

For details on the user interface, see “Regular Expression Tool” on page 232.

## 6 View Data from the Monitor in HP Business Availability Center

View the data in HP Business Availability Center:

- ▶ **Events integration.** If you chose and edited the Events script in the Field Mapping area, you can view events in Dashboard, System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- ▶ **Tickets integration.** If you chose and edited the tickets script in the Field Mapping area, you can view events in any application that supports SiteScope data, including SiteScope Over Time reports.
- ▶ **Measurements integration.** If you chose and edited the measurements script in the Field Mapping area, you can view the data in any application that supports SiteScope data, including SiteScope Over Time reports.
- ▶ If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <HP Business Availability Center root directory>\bin.

To troubleshoot problems with data arriving to HP Business Availability Center, see “Troubleshooting and Limitations” on page 1240.

## Technology Log File Integration Monitor User Interface

<p><b>Description</b></p>	<p>Technology Log File Integration Monitor watches for specific entries added to a log file of a Enterprise Management System (EMS) application by trying to match against a regular expression. From each matched entry, one sample is created and sent to HP Business Availability Center. Each time the monitor runs, it examines log entries added since the last time it ran.</p> <p>Use this page to add the monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “Integrate Log File Data into HP Business Availability Center” on page 1228</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Technology Log File Integration Monitor” on page 1225</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>



## Log File Integration Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Log file path name</b>	<p>Enter the path to the log file from which you want to extract data.</p> <ul style="list-style-type: none"> <li>▶ <b>Remote UNIX.</b> For reading log files on remote UNIX machines, the path must be relative to the home directory of UNIX user account being used to login to the remote machine. Select <b>Preferences &gt; UNIX Servers</b> for information about which UNIX user account is being used.</li> <li>▶ <b>Remote Windows NT/2000 through NetBIOS.</b> You can also monitor log files by including the UNC path to the remote log file. For example, <code>\\remoteserver\sharedfolder\filename.log</code>. This requires that the user account under which SiteScope is running has permission to access the remote directory using the UNC path. If a direct connection using the operating system is unsuccessful, SiteScope tries to match the <code>\\remoteserver</code> with servers currently defined as remote NT connection profiles (displayed in the Microsoft Windows remote server list). If an exact match is found for <code>\\remoteserver</code> in the remote NT connection profiles, SiteScope tries to use this connection profile to access the remote log file. If no matching server name is found, the monitor reports that the remote log file can not be found.</li> <li>▶ <b>Remote NT through SSH.</b> You must select the remote server using the <b>Server</b> selection above. It is not necessary to select a remote Windows server if you are using NetBIOS to connect to remote Windows servers.</li> </ul> <p>Optionally, you can use a regular expression to insert date and time variables. For example, you can use a syntax of <code>s/ex\$shortYear\$\$0month\$\$0day\$.log/</code> to match date-coded IIS log file names.</p>

GUI Element	Description
<b>Content match</b>	<p>Enter the text to look for in the log entries. You can also use a regular expression in this entry to match text patterns.</p> <p>Unlike the content match function of other SiteScope monitors, the Log File Monitor content match is run repeatedly against the most recent content of the target log file until all matches are found. This means the monitor not only reports if the match was found, but also how many times the matched pattern was found.</p> <p>To match text that includes more than one line of text, add an <code>s</code> search modifier to the end of the regular expression.</p>
<b>No error if file not found</b>	<p>Select if you want this monitor to remain in good status if the file is not found.</p>
<b>Log file encoding</b>	<p>If you are reading a log file whose encoding is different than the SiteScope machine's default encoding, select the log file encoding.</p> <p><b>Default value:</b> windows-1252</p>

GUI Element	Description
Run alerts	<p>Select the method for running alerts for this monitor:</p> <ul style="list-style-type: none"> <li>▶ Select <b>For each log entry matched</b> to trigger alerts for each matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error).           <p><b>Note:</b> When the Technology Log File Integration Monitor is run with this alert method selected, the monitor never displays an error or warning status in the SiteScope interface, regardless of the results of the content match or if the target log file is not found. The monitor triggers alerts if one or more matching entries are found and the Error if or Warning if thresholds are defined accordingly (for example, setting Error if to the default of matchCount &gt; 0).</p> </li> <li>▶ Select <b>Once, after all log entries have been checked</b> to count the number of matches and trigger alerts one time. The alert is based on the <b>Error if</b> and <b>Warning if</b> thresholds defined for the monitor.           <p><b>Note:</b> By default, selecting this option causes SiteScope to send one alert message if one or more matches are found, but the alert does not include any details of the matching entries. To have SiteScope include the matching entries, you must associate the monitor with an alert definition that has the property &lt;matchDetails&gt; in the alert template. This special template property is used to populate the alert with the details of all the matching entries. You use this for email alerts or other alert types that work with template properties.</p> <p>Email alert templates are stored in the &lt;SiteScope root directory&gt;\templates.mail directory.</p> </li> </ul>

GUI Element	Description
<b>EMS time difference</b>	<p>Enter a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded.</p> <p>You can also view the results of the test in the following log file: &lt;SiteScope root directory&gt;\logs\bac_integration.log.</p> <p><b>Note:</b> The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.</p>

### Field Mapping

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Sample Type</b>	<p>Select from the following sample types for this integration:</p> <ul style="list-style-type: none"> <li>▶ <b>Events.</b> For details, see “Configuring Field Mapping for Event Samples” on page 1150.</li> <li>▶ <b>Measurements.</b> For details, see “Configuring Field Mapping for Measurement Samples” on page 1156.</li> <li>▶ <b>Tickets.</b> For details, see “Configuring Field Mapping for Ticket Samples” on page 1159.</li> </ul>
<b>Load File</b>	Click to load the script that is applicable to the sample type selected above.

GUI Element	Description
<b>Field Mapping</b>	<p>The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring.</p> <p>The mapping is editable in this box. You can also copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1147.</p>
<b>Test Script</b>	<p>Click to test the field mapping script. We recommend that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: <b>&lt;SiteScope root directory&gt;\logs\bac_integration.log</b>.</p> <p><b>Note:</b> The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Topology Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Topology template</b>	<p>Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propagates its status to the CIs mapped in this topology.</p> <p>Select from:</p> <ul style="list-style-type: none"> <li>▶ <b>Custom.</b> You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or EMS monitor CIs.</li> <li>▶ <b>Hosts.</b> Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the topology.</li> <li>▶ <b>Hosts-Applications.</b> Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI as leaf nodes of the application CI. The host CI also has an EMS monitor CI as a leaf node.</li> </ul> <p><b>Note:</b> We recommend not to select <b>Custom</b> as this does not load a script and you must enter the entire script yourself. We recommend that you begin with either <b>Host</b> or <b>Host and Application</b> and edit one of those scripts.</p> <p>For more details, see “Topology Settings for Technology Integration Monitors” on page 1133.</p>
<b>Load Script</b>	<p>Click to load the required Jython script for the topology you selected in the <b>Topology template</b> option. If you selected <b>Custom</b>, there is no script to load.</p>

GUI Element	Description
<b>Script</b>	<p>The contents of the script are editable in this box. However, we recommend not to edit the contents of the script here. You can copy the contents of the script into your preferred text edit, edit the script as needed, and then copy the contents back into this box.</p> <p><b>Note:</b> The Jython script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see “Topology Settings for Technology Integration Monitors” on page 1133.</p>
<b>Test Script</b>	<p>Click to test the topology script. It is recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is mapped. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: &lt;SiteScope root directory&gt;\logs\bac_integration.log.</p> <p><b>Note:</b> The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Troubleshooting and Limitations

- ▶ Check for errors in `<SiteScope root directory>\logs\RunMonitor.log` and in `<SiteScope root directory>\logs\error.log`.
- ▶ Change the log level to DEBUG in `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties`, to watch outgoing samples.

Change the line:

```
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
```

to:

```
log4j.category.EmsEventPrinter= DEBUG, ems.appender.
```

The log file to look at is:

```
<SiteScope root directory>\logs\RunMonitor.log
```

- ▶ If samples are created and sent from SiteScope, but the data is not seen in **Dashboard/Event Log/SiteScope reports**, look in `<HP Business Availability Center root directory>\log\mercury_wde\wdeIgnoredSamples.log` to make sure the samples were not dropped due to missing fields or values.
- ▶ Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine:  
`<HP Business Availability Center root directory>\conf\core\tools\log4j\mercury_wde\wde.properties`

Change the log level parameter to DEBUG in the following lines:

- ▶ `log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender`
- ▶ `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender`

Look at the corresponding log files:

- ▶ `<HP Business Availability Center root directory>\logs\mercury_wde\wdeIgnoredSamples.log`
- ▶ `<HP Business Availability Center root directory>\logs\mercury_wde\wdePublishedSamples.log`



# 110

---

## Technology SNMP Trap Integration Monitor

The Technology SNMP Trap Integration Monitor watches for SNMP traps received by SiteScope from third-party Enterprise Management Systems (EMS). For each SNMP trap that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the SNMP trap values.

The third-party EMS systems must be configured to send traps to the SiteScope server.

### **This chapter includes:**

#### Concepts

- ▶ Technology SNMP Trap Integration Monitor Overview on page 1242

#### Tasks

- ▶ Integrate SNMP Trap Data into HP Business Availability Center on page 1243

#### Reference

- ▶ Technology SNMP Trap Integration Monitor Settings on page 1247

**Troubleshooting and Limitations** on page 1253

## **Technology SNMP Trap Integration Monitor Overview**

The Technology SNMP Trap Integration Monitor is useful for integrating traps that your external devices create into the HP Business Availability Center framework. For example, you can use this monitor to forward information from Hewlett Packard Network Node Manager to Business Availability Center. See “Integration with HP Network Node Manager” on page 1269 for more information.

This section also includes:

- ▶ “What Data Is Collected” on page 1242
- ▶ “Configuring the Monitor” on page 1242

### **What Data Is Collected**

The Technology SNMP Trap Integration Monitor collects data that is extracted from any SNMP trap (version 1 and 2) received by SiteScope and sends notifications to HP Business Availability Center containing preferred values from the original SNMP trap.

Before setting up the Technology SNMP Trap Integration Monitor, you should be clear about the purpose and usage of the data in HP Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

The specific data that is forwarded to HP Business Availability Center is controlled by the field mapping script. You use this script to specify the preferred value fields that you want forwarded. For more details on selecting the script and the file structure and syntax, see “Integration Monitor Field Mapping” on page 1147.

### **Configuring the Monitor**

For task details, see “Integrate SNMP Trap Data into HP Business Availability Center” on page 1243.

For user interface details, see “Technology SNMP Trap Integration Monitor Settings” on page 1247.

## Integrate SNMP Trap Data into HP Business Availability Center

This section provides the overall flow for setting up the Technology SNMP Trap Integration Monitor to work with HP Business Availability Center. If you need more information on performing any of the steps, see the section on “Technology SNMP Trap Integration Monitor Settings” on page 1247.

This task includes the following steps:

- “Prerequisites” on page 1243
- “Configure the Relevant Software to Send SNMP Traps to the SiteScope Machine.” on page 1243
- “Use SiteScope SNMP Trap Tool to Watch If the Traps Are Received” on page 1244
- “Create a Technology SNMP Trap Integration Monitor” on page 1244
- “Edit the Monitor’s Field Mappings” on page 1245
- “Edit the Monitor’s Topology Settings - Optional” on page 1246
- “View Data from the Monitor in HP Business Availability Center” on page 1246

### **1 Prerequisites**

Your SiteScope has to be integrated with Business Availability Center and enabled to forward data.

For details on how to perform this task, see “Collect Data on the Performance of an IT Resource” on page 164.

### **2 Configure the Relevant Software to Send SNMP Traps to the SiteScope Machine.**

The SNMP agents you want to monitor must be configured to send SNMP traps to the SiteScope host. Consult with the system administrator or applicable product documentation for more about SNMP configuration.

### 3 Use SiteScope SNMP Trap Tool to Watch If the Traps Are Received

If you do not see any traps, make sure that the SNMP trap port is available for the SiteScope. The Technology SNMP Trap Integration Monitor uses port 162 for receiving traps.

- a Stop the SiteScope service.
- b Verify that the SNMP trap port (162) is available—`netstat -na | find "162"` shows no output.
- c If the port is busy, locate the process or program that uses it (for example the Microsoft SNMP Trap Service) and terminate it.

**Note:** To see which process uses this port, you can download `tcpview` from [www.sysinternals.com](http://www.sysinternals.com).

- d Restart SiteScope.

### 4 Create a Technology SNMP Trap Integration Monitor

Add a Technology SNMP Trap Integration Monitor to SiteScope. For details on the user interface, see “Technology SNMP Trap Integration Monitor Settings” on page 1247.

- When adding the new monitor to a group, it is recommended that you use a dedicated group for integration monitors only.
- If you do not see the **Integration Monitors** category, make sure you have an EMS Option License for your SiteScope.
- **Name.** It is recommended that the monitor name include the name of the integrated software.

## 5 Edit the Monitor's Field Mappings

In the New Technology SNMP Trap Integration Monitor dialog box, expand the Field Mapping area. Select a field mapping type and click **Load Script**.

---

**Note:** If you are configuring a Netuitive integration, do not click **Load Script**. You must copy the contents of the file already configured for this integration into the Field Mapping area. For details, see “Display Netuitive SI Data in Dashboard” on page 611 in *Solutions and Integrations*.

---

- ▶ If you select **Events** or **Metrics**, a template script is displayed in the **Field mapping** box. Edit the script to enable SiteScope to retrieve the data from the monitored application that you want to forward to Business Availability Center.
- ▶ If you select **Custom**, create your own script to map the fields for retrieving data from the monitored application.

---

**Note:** All the received traps are saved to **snmptrap.log** in **<SiteScope root directory>\logs**. When referring to data arriving from the Technology SNMP Trap Integration Monitor, use the names from the snmptrap.log file, prefixed with the dollar sign (\$).

For example:

Use the \$oid to refer to the oid value of the trap, \$var1 to refer to the variable bound as the first variable in trap, and \$var2 for variable bound as second variable in trap.

---

For details on working with the field mapping script, see “Integration Monitor Field Mapping” on page 1147.

For details on the user interface, see “Field Mapping” on page 1249.

## 6 Edit the Monitor's Topology Settings - Optional

Optionally, in the New Technology SNMP Trap Integration Monitor dialog box in the Topology Settings area, you can create a Jython script that creates a topology of configuration items in HP Business Availability Center's CMDB to match your EMS system. You copy the script into the Script field in the Topology Settings.

For details on this topic, see “Topology Settings for Technology Integration Monitors” on page 1133.

For details on the user interface, see “Topology Settings” on page 1251.

## 7 View Data from the Monitor in HP Business Availability Center

View the data in HP Business Availability Center:

- ▶ You can view SNMP traps in the **Tools** link or in <SiteScope root directory>\logs\snmptrap.log. (For a better understanding of what SNMP traps are, refer to: [www.snmpblink.org](http://www.snmpblink.org).)
- ▶ **Events integration.** If you chose and edited the Events script in the Field Mapping area, you can view events in Dashboard, System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- ▶ **Metrics integration.** If you chose and edited the Metrics script in the Field Mapping area, you can view the data in any application that supports SiteScope data, including SiteScope Over Time reports.
- ▶ If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <HP Business Availability Center root directory>\bin.

To troubleshoot problems with data arriving to HP Business Availability Center, see “Troubleshooting and Limitations” on page 1253.

## Technology SNMP Trap Integration Monitor Settings

<p><b>Description</b></p>	<p>The Technology SNMP Trap Integration Monitor watches for SNMP traps received by SiteScope from third-party Enterprise Management Systems (EMS).</p> <p>For each SNMP trap that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the SNMP trap values.</p> <p>The third-party EMS systems must be configured to send traps to the SiteScope server.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ Monitors must be created in a group in the monitor tree.</li> <li>▶ The <b>SNMP Trap Tool</b> is available when configuring this monitor to view SNMP Traps received by SiteScope's SNMP listener (provided you are an administrator in SiteScope, or a user granted <b>Use monitor tools</b> permissions). To use the tool when configuring or editing a monitor, click the <b>Use Tool</b> button. For details on the tool, see “SNMP Trap Tool” on page 243.</li> </ul>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “Integrate SNMP Trap Data into HP Business Availability Center” on page 1243</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Technology SNMP Trap Integration Monitor” on page 1241</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Technology SNMP Trap Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<p><b>Run alerts</b></p>	<p>Choose the method for running alerts:</p> <ul style="list-style-type: none"> <li>➤ If <b>For each SNMP Trap received from EMS system</b> is chosen, then the monitor triggers alerts for every matching entry found. When the Technology SNMP Trap Integration Monitor is run in the for each SNMP Trap received from EMS system alert method, the monitor never reports a status of error or warning, regardless of the results of the content match or even if the target SNMP Trap is not found.</li> <li>➤ If <b>Once, after all SNMP Traps from EMS system were received</b> is chosen, then the monitor counts up the number of matches and triggers alerts based on the Error If and Warning If thresholds defined for the monitor in the Advanced Settings section.</li> </ul>
<p><b>EMS time difference</b></p>	<p>Enter a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded.</p> <p><b>Note:</b> The time difference value only needs to be entered if the difference is greater than one minute. There is no need to synchronize differences of seconds less than one minute.</p>



## Field Mapping

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Sample Type</b>	<p>Select from the following sample types for this integration:</p> <ul style="list-style-type: none"> <li>▶ <b>Events.</b> For details, see “Configuring Field Mapping for Event Samples” on page 1150.</li> <li>▶ <b>Measurements.</b> For details, see “Configuring Field Mapping for Measurement Samples” on page 1156.</li> <li>▶ <b>Tickets.</b> For details, see “Configuring Field Mapping for Ticket Samples” on page 1159.</li> </ul>
<b>Load File</b>	<p>Click to load the script that is applicable to the sample type selected above.</p>
<b>Field mapping</b>	<p>The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring.</p> <p>The mapping itself is not editable in the UI. You must copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1147.</p>

GUI Element	Description
<b>Test Script</b>	<p>Click to test the field mapping script. We recommend that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: &lt;SiteScope root directory&gt;\logs\bac_integration.log.</p> <p><b>Note:</b> The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Topology Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Topology template</b>	<p>Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propagates its status to the CIs mapped in this topology.</p> <p>Select from:</p> <ul style="list-style-type: none"> <li>▶ <b>Custom.</b> You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or EMS monitor CIs.</li> <li>▶ <b>Hosts.</b> Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the topology.</li> <li>▶ <b>Hosts-Applications.</b> Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI as leaf nodes of the application CI. The host CI also has an EMS monitor CI as a leaf node.</li> </ul> <p><b>Note:</b> We recommend not to select <b>Custom</b> as this does not load a script and you must enter the entire script yourself. We recommend that you begin with either <b>Host</b> or <b>Host and Application</b> and edit one of those scripts.</p> <p>For more details, see “Topology Settings for Technology Integration Monitors” on page 1133.</p>
<b>Load Script</b>	<p>Click to load the required Jython script for the topology you selected in the <b>Topology template</b> option. If you selected <b>Custom</b>, there is no script to load.</p>

GUI Element	Description
<p><b>Script</b></p>	<p>The contents of the script are visible in this box. However, we recommend not to edit the contents of the script here. You must copy the contents of the script into your preferred text edit, edit the script as needed, and then copy the contents back into this box.</p> <p><b>Note:</b> The Jython script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see “Topology Settings for Technology Integration Monitors” on page 1133.</p>
<p><b>Test Script</b></p>	<p>Click to test the topology script. We recommend that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is mapped. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: &lt;SiteScope root directory&gt;\logs\bac_integration.log.</p> <p><b>Note:</b> The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Troubleshooting and Limitations

The following sections provide information on troubleshooting for the Technology SNMP Trap Integration Monitor, and verifying the communication paths:

- ▶ “Basic Troubleshooting Guidelines” on page 1253
- ▶ “Verify SNMP Trap Reception to SiteScope” on page 1254
- ▶ “Common Problems and Solutions” on page 1255

### Basic Troubleshooting Guidelines

- ▶ Check for errors in `<SiteScope root directory>\logs\RunMonitor.log` and in `<SiteScope root directory>\logs\error.log`.
- ▶ Change the log level to DEBUG in `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties`, to watch outgoing samples.

Change the line:

```
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
to:
```

```
log4j.category.EmsEventPrinter= DEBUG, ems.appender.
```

The log file to look at is: `<SiteScope root directory>\logs\RunMonitor.log`

- ▶ Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine: `<HP Business Availability Center root directory>\conf\core\tools\log4j\mercury_wde\wde.properties`

Change the log level parameter to DEBUG in the following lines:

- ▶ `log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender`
- ▶ `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender`

Refer to the following log files:

- ▶ <HP Business Availability Center root directory>\logs\mercury\_wde\wdeIgnoredSamples.log
- ▶ <HP Business Availability Center root directory>\logs\mercury\_wde\wdePublishedSamples.log

## **Verify SNMP Trap Reception to SiteScope**

You can verify that SiteScope is receiving SNMP traps from other management systems using the SiteScope SNMP Trap Monitor. Use the following steps to verify that SiteScope is receiving traps.

**To verify that SiteScope is receiving SNMP traps:**

- 1** Configure the intended SNMP Trap sending entity to send traps to the SiteScope machine. The steps to configure the SNMP host depends on system. Usually, it involves lowering system thresholds to cause normal situations to create traps. On some systems there is a test mode that you can use to create traps on demand. The other way is to use one of the freely available SNMP trap generators, and to send copies of the trap to SiteScope.
- 2** Inspect the SNMP Trap Monitor log file in SiteScope for sent traps. Every SNMP Trap received by the SiteScope is written into the SNMP Trap Monitor's log file, located in <SiteScope root directory>\logs\snmptrap.log.

## Common Problems and Solutions

The following table summarizes common problems and suggested solutions:

Problem Symptom	Possible Cause	Solution
The monitor does not appear in the monitor list.	Option License for Integration Monitors had not been provided.	Provide the Option License for Integration Monitors.
The monitor reports an Address in use error and the monitor type is unavailable.	Another application or process on the machine where SiteScope is running has bound the port 162, the port used to receive SNMP traps.	You must stop the SiteScope service, terminate the process or service that is using the port, and restart SiteScope.

Problem Symptom	Possible Cause	Solution
<p>The SNMP traps are not forwarded to HP Business Availability Center applications.</p>	<p>The SNMP Agent does not emit SNMP traps.</p>	<p>Verify that the SNMP Agent is configured to emit SNMP traps. Use the <code>&lt;SiteScope&gt;\logs\snmptrap.log</code> file to verify that traps are received by SiteScope. For details, see “Verify SNMP Trap Reception to SiteScope” on page 1254.</p>
	<p>The EMS configuration file contains errors.</p>	<p>Click the <b>Test Script</b> button in the Field Mapping area to verify the field mapping.</p>
	<p>The SNMP trap port is busy.</p>	<p>Make sure that no other SNMP trap service is listening to SNMP traps on the SiteScope machine. Microsoft SNMP Trap Service is common cause on computers running Windows NT or Windows 2000 operating system.</p>
	<p>The monitor is not configured to report to these applications.</p>	<p>Make sure that the monitor is configured to report to these applications.</p>
<p>Samples are created and sent from SiteScope, but the data is not seen in Dashboard/Event Log/SiteScope reports.</p>	<p>Samples were dropped due to missing fields or values.</p>	<p>Check in <code>&lt;HP Business Availability Center root directory&gt;\log\mercury_wde\wdeIgnoredSamples.log</code>.</p>



## Technology Web Service Integration Monitor

The Technology Web Service Integration Monitor enables a Web service entry point to SiteScope. The monitor can be used to report data from third-party Enterprise Management Systems (EMS) to SiteScope through Web service. Both event and metrics entry points into HP Business Availability Center are published for external systems to use. For each event and/or metric that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the event and/or metrics values.

### **This chapter includes:**

#### **Concepts**

- ▶ Technology Web Service Integration Monitor Overview on page 1258

#### **Tasks**

- ▶ Check Connectivity to the Technology Web Service Integration Monitor on page 1261

#### **Reference**

- ▶ Technology Web Service Integration Monitor Settings on page 1262

#### **Troubleshooting and Limitations on page 1267**

## **Technology Web Service Integration Monitor Overview**

Use the Technology Web Service Integration Monitor for integrating event data or metrics data from your existing EMS system to HP Business Availability Center. SiteScope supplies a WSDL file which the user can use to create a client code. The client code reports the event and/or metrics data to SiteScope. The client has several ways to report data to HP Business Availability Center:

- report one event
- report an array of events
- report one metric
- report an array of metrics

This section includes the following topics:

- “What Data Is Collected” on page 1258
- “Limitations” on page 1259
- “Setup Requirements” on page 1259
- “Configuring the Monitor” on page 1260

### **What Data Is Collected**

The Technology Web Service Integration Monitor collects data that is extracted from any message received by SiteScope report data Web service and sends notifications to HP Business Availability Center containing preferred values from the original message.

Before setting up the Technology Web Service Integration Monitor, you should understand and map out the purpose and usage of the data that is forwarded to HP Business Availability Center. You should determine if the data is for presentation in the Dashboard, Service Level Management, and/or reports.

The specific data that is forwarded to HP Business Availability Center is controlled by the field mapping script. You use this script to specify the preferred value fields that you want forwarded. For more details on selecting the script and the file structure and syntax, see “Integration Monitor Field Mapping” on page 1147.

## Limitations

If you are working with HP Business Availability Center version 5.1 and lower, you cannot define new Technology Web Service Integration monitors or edit existing ones from within HP Business Availability Center. If you need to define a new Technology Web Service Integration monitor or edit an existing monitor, detach SiteScope from HP Business Availability Center, define the monitor in SiteScope’s new user interface, and then attach the SiteScope to HP Business Availability Center again.

## Setup Requirements

- ▶ When adding the monitor to SiteScope, in the Field Mapping panel, you must select a field mapping script and load the script for the monitor. Copy the contents of the script into your preferred text editor and edit the script to define the event handlers for the monitor instance. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 1147.
- ▶ To enable the connection to SiteScope reportMonitorData Web service, you must create a client code (in any language) that makes the connection and handles the reporting of the data to SiteScope through the Web service. For details on enabling the connection, see below.

**To enable the connection to SiteScope reportMonitorData Web service:**

- 1** Open Explorer and go to SiteScope (<http://<SiteScope host>:8080/SiteScope/services>). Take the WSDL file of the service **reportMonitorData**. The WSDL is an interface file which represents the API of the reportMonitorData Web service in SiteScope. The reportMonitorData service is the service that listens to incoming messages and forwards them to HP Business Availability Center. This file is used to create the client stubs that connect to the service and report the data.
- 2** Generate the stubs using the WSDL file. The generation of the stubs can be to any language. The way to create the files depends on the language that you want to use.

For example, if you want to use Java as the client code, you must use the WSDL2JAVA task in AXIS package that can be downloaded from their Web site. Run **Java org.apache.axis.wsdl.WSDL2Java <name of saved WSDL file>**. After running this, you get two packages. One package is **com**, which holds the needed objects for sending the data, and the second is **localhost**, which holds the stubs that makes the connection to SiteScope Web service.

- 3** Write the actual client code which uses the generated classes to send the data to SiteScope. In the code, call the **setreportMonitorDataEndpointAddress(<SiteScope targetHost>)**, which is found in **MonitorDataAcceptorServiceLocator** (one of the generated stubs) to set the SiteScope address to where you want the data reported.
- 4** Run your code and check if you get data in the SiteScope Technology Web Service Integration monitor.

## **Configuring the Monitor**

For task details, see “Check Connectivity to the Technology Web Service Integration Monitor” on page 1261.

For user interface details, see “Technology Web Service Integration Monitor Settings” on page 1262.

## Check Connectivity to the Technology Web Service Integration Monitor

After creating a Technology Web Service Integration monitor in SiteScope, you can check connectivity to the Web service by using the **test\_client** which is located in the <SiteScope root directory>\conf\ems\webservice\test\_client directory. This tool sends constant messages to SiteScope reportMonitorData Web service. The messages can be either metrics messages or event messages.

**To use the client tool to check connectivity:**

- 1** In the <SiteScope root directory>\conf\ems\webservice\test\_client directory, run the **test\_event\_client.bat** for events or **test\_metrics\_client.bat** for metrics, using the following parameters:
  - ▶ **Target Host.** The address of the SiteScope host which receives the messages.
  - ▶ **Number of messages to send.** Number of messages to send to SiteScope.
  - ▶ **System Id.** System Id of the monitor that receives the messages.
  - ▶ **Severity/Quality.** Severity of the event when forwarding events (default is to send 1 to 5). Quality of the metric when forwarding metrics data (default is 0-3).
- 2** If you are forwarding other values to HP Business Availability Center, you must edit the field mapping accordingly.

The tool can also be run with no parameters. In this case, the tool tries to send one message to the local host. The message has the system id: **Test Event System Id**. The severity is 5 (for events) or the quality is 3 (for metrics).

If you use this option, you must activate it on the SiteScope machine and add a Technology SNMP Trap Integration monitor with the system id: **Test Event System Id**.

- 3** After running the tool, go to the required SiteScope monitor and see if the number of messages received equals the number that you sent. In addition, you can go to one of the applications (Dashboard, System Availability Management) and see if the data that you sent is displayed.

## Technology Web Service Integration Monitor Settings

<p><b>Description</b></p>	<p>The Technology Web Service Integration Monitor enables a Web service entry point to SiteScope. The monitor can be used to report data from third-party Enterprise Management Systems (EMS) to SiteScope through Web service. Both event and metrics entry points into HP Business Availability Center are published for external systems to use. For each event and/or metric that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the event and/or metrics values.</p> <p>Use this page to add the monitor or edit the monitor's properties.</p> <p><b>To access:</b> Select the <b>Monitors</b> context. In the monitor tree, right-click a group, select <b>New &gt; Monitor</b>, and select the monitor from the New Monitor Page.</p>
<p><b>Important Information</b></p>	<p>Monitors must be created in a group in the monitor tree.</p>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “Check Connectivity to the Technology Web Service Integration Monitor” on page 1261</li> <li>▶ “Deploy a Monitor – Workflow” on page 323</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Technology Web Service Integration Monitor” on page 1257</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Technology Web Service Integration Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>System ID</b>	<p>Enter a text system id for the Technology Web Service Integration Monitor instance.</p> <p>Each received message from the EMS system holds a system id. Each monitor receives messages only with a system id that matches the system id defined in the monitor. The system id is unique for all monitors. Enter the system id that represents the messages that you want this monitor to receive.</p>

## Field Mapping

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Sample Type</b>	<p>Select from the following sample types for this integration:</p> <ul style="list-style-type: none"> <li>▶ <b>Events.</b> For details, see “Configuring Field Mapping for Event Samples” on page 1150.</li> <li>▶ <b>Measurements.</b> For details, see “Configuring Field Mapping for Measurement Samples” on page 1156.</li> <li>▶ <b>Tickets.</b> For details, see “Configuring Field Mapping for Ticket Samples” on page 1159.</li> </ul>
<b>Load File</b>	<p>Click to load the script that is applicable to the sample type selected above.</p>

GUI Element	Description
<p><b>Field Mapping</b></p>	<p>The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring.</p> <p>The mapping itself is not editable in the UI. You must copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p>For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 1147.</p>
<p><b>Test Script</b></p>	<p>Click to test the field mapping script. We recommend that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: <b>&lt;SiteScope root directory&gt;\logs\bac_integration.log</b>.</p> <p><b>Note:</b> The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>



## Topology Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Topology template</b>	<p>Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propagates its status to the CIs mapped in this topology.</p> <p>Select from:</p> <ul style="list-style-type: none"> <li>▶ <b>Custom.</b> You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or EMS monitor CIs.</li> <li>▶ <b>Hosts.</b> Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the topology.</li> <li>▶ <b>Hosts-Applications.</b> Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI as leaf nodes of the application CI. The host CI also has an EMS monitor CI as a leaf node.</li> </ul> <p><b>Note:</b> We recommend not to select <b>Custom</b> as this does not load a script and you must enter the entire script yourself. We recommend that you begin with either <b>Host</b> or <b>Host and Application</b> and edit one of those scripts.</p> <p>For more details, see “Topology Settings for Technology Integration Monitors” on page 1133.</p>
<b>Load Script</b>	<p>Click to load the required Jython script for the topology you selected in the <b>Topology template</b> option. If you selected <b>Custom</b>, there is no script to load.</p>

GUI Element	Description
<b>Script</b>	<p>The contents of the script are visible in this box. However, we recommend not to edit the contents of the script here. You must copy the contents of the script into your preferred text edit, edit the script as needed, and then copy the contents back into this box.</p> <p><b>Note:</b> The Jython script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see “Topology Settings for Technology Integration Monitors” on page 1133.</p>
<b>Test Script</b>	<p>Click to test the topology script. We recommend that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is mapped. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period.</p> <p>You can also view the results of the test in the following log file: &lt;SiteScope root directory&gt;\logs\bac_integration.log.</p> <p><b>Note:</b> The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Troubleshooting and Limitations

- ▶ Check for errors in **<SiteScope root directory>\logs\RunMonitor.log** and in **<SiteScope root directory>\logs\error.log**.
- ▶ Change the log level to DEBUG in **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties**, to watch outgoing samples.

Change the line:

```
log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
to:
```

```
log4j.category.EmsEventPrinter= DEBUG, ems.appender.
```

The log file to look at is:

**<SiteScope root directory>\logs\RunMonitor.log**

- ▶ If samples are created and sent from SiteScope, but the data is not seen in **Dashboard/Event Log/SiteScope reports**, look in **<HP Business Availability Center root directory>\log\mercury\_wde\wdeIgnoredSamples.log** to make sure the samples were not dropped due to missing fields or values.
- ▶ Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine: **<HP Business Availability Center root directory>\conf\core\tools\log4j\mercury\_wde\wde.properties**

Change the log level parameter to DEBUG in the following lines:

- ▶ `log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender`
- ▶ `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender`

Look at the corresponding log files:

- ▶ **<HP Business Availability Center root directory>\logs\mercury\_wde\wdeIgnoredSamples.log**
- ▶ **<HP Business Availability Center root directory>\logs\mercury\_wde\wdePublishedSamples.log**



# 112

---

## Integration with HP Network Node Manager

HP Business Availability Center can accept events from Hewlett-Packard Network Node Manager (NNM).

### **This chapter includes:**

#### Concepts

- ▶ Network Node Manager Integration Overview on page 1269
- ▶ Writing Scripts to Export Network Node Manager Data on page 1270

#### Tasks

- ▶ Configure Events in Network Node Manager on page 1271

### **Network Node Manager Integration Overview**

You can forward from Network Node Manager (NNM) event data by configuring NNM to run a script for each event that you want forwarded to HP Business Availability Center. The script that you write and associate with NNM can do one of the following actions:

- ▶ write the NNM data to a log file
- ▶ send an SNMP trap with the NNM data to a SiteScope server

If your script writes the data to a log you then use a Technology Log File Integration Monitor to read the data and forward it to HP Business Availability Center. If you use a script to send an SNMP trap to a SiteScope server, you use an Technology SNMP Trap Integration Monitor configured to receive it and forward to HP Business Availability Center.

## Writing Scripts to Export Network Node Manager Data

The script you use should accept data from Network Node Manager as a command line argument, and process the data so that it can be forwarded to HP Business Availability Center. The following sections describe example scripts that can be used to export NNM data.

This section includes the following topics:

- ▶ “Sample Script for Writing to a Log File” on page 1270
- ▶ “Sample Script for Sending SNMP Trap Data” on page 1270

### **Sample Script for Writing to a Log File**

The following Perl script receives data from the command line and writes it to a log file as a comma separated vector of values that can be parsed by the Log File Integration Monitor:

```
#!/usr/bin/perl
open LOG, ">>log1.log" or die;
print LOG (join ', ', @ARGV) . "\n";
close LOG;
```

### **Sample Script for Sending SNMP Trap Data**

The following Perl script receives data from the command line and sends it as a message in an SNMP trap (using SNMP data generated by Network Node Manager) that can be caught by a Technology SNMP Trap Integration Monitor. It accepts the host name to which the trap is sent as the first parameter and a string description of the alert as the second parameter.

```
#!/usr/bin/perl
$host = $ARGV[0];
$message = $ARGV[1];
system("snmptrap $host \"\ \" \" 6 0 5 system.sysDescr.0 \" . \"octetstringasci
$message");
```

## **Configure Events in Network Node Manager**

Use the following steps to configure Network Node Manager to run a script for the requested events in Network Node Manager. The figure below shows examples of the applicable Network Node Manager pages and dialogs you use.

**To configure Network Node Manager to run scripts:**

- 1** From the **Options** menu choose **Event Configuration**.
- 2** Select the requested enterprise and event from the **Event Configuration** dialog.
- 3** Select the Actions tab from the Edit > Events > Modify Events dialog.
- 4** Enter the command line for the script in the **Command for Automatic Action** text box. You may use NNM variables to pass data to the command line.
- 5** Click **OK** to close the **Modify Events** dialog.
- 6** From the **File** menu in the **Event Configuration** dialog select **Save**.





# Part V

---

## Remote Servers



# 113

---

## Working with Remote Servers

This chapter includes the main concepts, tasks, and reference information for configuring SiteScope to monitor data on remote servers.

### **This chapter includes:**

#### Concepts

- ▶ Remote Servers Overview on page 1276

#### Tasks

- ▶ Configure SiteScope to Monitor a Remote Microsoft Windows Server on page 1277
- ▶ Configure SiteScope to Monitor a Remote UNIX Server on page 1285

#### Reference

- ▶ Remote Servers User Interface on page 1287
- ▶ Troubleshooting and Limitations on page 1309

## Remote Servers Overview

SiteScope must be able to establish a connection to the servers you want to monitor. It must also be authenticated as a user having account permissions to access the Windows performance registry on the Windows remote machine and to run command line tools on the UNIX remote machine as a remote user.

Windows/UNIX Remote server options are used to set up the connection properties, such as credentials and protocols, so that SiteScope can monitor systems and services running in remote environments. You can then create monitors to watch the resources and performance counters for that server. Multiple monitors can use the same connection profile. You can also create multiple remote servers for the same host machine.

---

**Note:** If multiple Windows remote servers are configured for the same host machine using the NetBIOS method, the connection fails. This is because Windows NT does not allow multiple connections to a server or shared resource by the same user, using more than one user name (System error 1219).

---

For details on enabling SiteScope to monitor data on remote servers, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277 and “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285.

For details on configuring these settings in the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291 and “New/Edit UNIX Remote Servers Dialog Box” on page 1299.

For information about troubleshooting and limitations of SiteScope monitoring of remote servers, see “Troubleshooting and Limitations” on page 1309.

---

**Note:** You can use SiteScope UNIX operating system adapters to extend SiteScope to connect to, and remotely monitor versions of UNIX that are not supported by default. For details, see “UNIX Operating System Adapters” on page 1363.

---

## **Configure SiteScope to Monitor a Remote Microsoft Windows Server**

This task describes the steps involved in configuring SiteScope to monitor data on remote Windows servers.

This task includes the following steps:

- “Enable SiteScope to Monitor Data on Remote Windows Servers” on page 1278
- “Configure User Permissions for Remote Monitoring” on page 1278
- “Configure and Test the Settings for the Windows Remote Server” on page 1278
- “Results” on page 1279

## 1 Enable SiteScope to Monitor Data on Remote Windows Servers

To enable SiteScope to monitor data on remote Windows servers, you must perform one of the following steps:

- ▶ Define an individual remote Windows server connection profile for each server. For details on how to perform this task, see “Define Remote Windows Server Connection Profiles” on page 1280.
- ▶ Set domain access privileges to permit SiteScope to access remote servers. For details on how to perform this task, see “Set Domain Privileges for SiteScope Monitoring” on page 1280.

## 2 Configure User Permissions for Remote Monitoring

Configure the user permissions to access the remote machine according to the operating system on the SiteScope machine. For details on how to perform this task, see “Configure User Permissions for Remote Monitoring” on page 1282.


## 3 Configure and Test the Settings for the Windows Remote Server

- a Configure the remote Windows server in the remote server tree. For details on the user interface, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.

---

### Note:

- ▶ If WMI is selected as the method for gathering management data from remote servers in the Main Settings **Method** field, the WMI service must be configured on the remote machine. For details on how to perform this task, see “Configure the WMI Service for Remote Monitoring” on page 1284.
  - ▶ If you are configuring remote Windows Servers for SSH monitoring with SiteScope, see “Configure Remote Windows Servers for SSH monitoring” on page 1325.
-

- b** After defining the Microsoft Windows remote server definition for SiteScope, click the **Test**  button for the applicable server to test the connection.

---

**Note:**

- ▶ If an "unable to connect to remote machine" error message opens when trying to view remote counters, refer to the Microsoft Knowledge Base (<http://support.microsoft.com/kb/300702/>).
  - ▶ Testing SSH connectivity to a remote Windows server using the Plink connection method for key-based Authentication returns a success message even if the test fails.
- 

## 4 Results

The server is added to the list of remote Windows Remote servers in the remote server tree. You can then create monitors to watch the resources and performance counters for that server. Multiple monitors can use the same connection profile.



## **Define Remote Windows Server Connection Profiles**

Monitoring remote Windows server data requires authenticated access to the remote server. A Windows server connection profile provides the necessary address and login credentials for SiteScope to log on to a remote server and to access the Windows performance registry on that remote machine.

**To log on to a remote server using the Windows server connection profile, either:**

- ▶ Log on to the remote server as a user with administrator privileges, or
- ▶ Create or modify a user account on the remote server that corresponds with the connection method and login permissions used in the SiteScope connection profile for that server.

## **Set Domain Privileges for SiteScope Monitoring**

SiteScope for Windows automatically generates a list of servers visible in the local domain. These servers are listed in the Servers list for monitor types where a server must be specified. SiteScope running on Windows may be able to use this list to monitor remote Windows servers without having to create individual connection profiles for each server.

**To set domain privileges, use one of the following methods:**

- ▶ **Set the SiteScope service to run as a user in the Domain Admin group.**

By default, SiteScope is installed to run as a Local System account. You can set the SiteScope service to log on as a user with domain administration privileges. This gives SiteScope access privileges to monitor server data within the domain. For details on how to change the SiteScope account user, see “Change the User Account of the SiteScope Service” on page 1281.

- ▶ **Add the server where SiteScope is running to the Domain Admin group in ActiveDirectory (for Windows 2000 or later).**

With this option, the SiteScope service is set to log on as a Local System account, but the machine where SiteScope is running is added to a group having domain administration privileges.



- **Edit the registry access permissions for all machines in the domain to allow non-admin access.**

This option requires changes to the registry on each remote machine that you want to monitor. This means that while the list of servers in the domain includes all machines in the domain, only those remote machines whose registry has been modified can be monitored without use of a connection profile.



### **Change the User Account of the SiteScope Service**

This task describes the steps involved in changing the user account of the SiteScope service.

**To change the user account of the SiteScope service:**

- 1** Select **Start > Programs > Administrative Tools > Services**, and select **SiteScope** from the list of services. The SiteScope Properties dialog box opens.
- 2** Click the **Log On** tab, and in the **Log on as** area, enter an account that can access the remote servers.
- 3** Click **OK** to save your settings and close the SiteScope Properties dialog box.
- 4** Right-click **SiteScope**. Click **Stop** to stop the SiteScope service.
- 5** Click **Start**. The SiteScope service now uses the new account.

## **Configure User Permissions for Remote Monitoring**

For SiteScope to collect performance measurements on a remote machine, SiteScope must have permission to access the remote machine. This task describes how to configure user permissions according to the operating system on the SiteScope machine.

---

### **Note:**

- ▶ Microsoft Best Practice recommends giving permissions to groups instead of to users.
  - ▶ Back up the registry before making any registry changes.
- 

### **To configure Windows XP and Windows 2003:**

- 1** On the SiteScope machine, select **Start > Run**. In the Open text box, enter **Regedt32.exe**. The Registry Editor dialog box opens.
- 2** In the **HKEY\_LOCAL\_MACHINE** window, select **SOFTWARE > Microsoft > Windows NT > CurrentVersion > Perflib**.
- 3** Click **Security** in the Registry Editor tool bar and select **Permissions**. The Permissions for Perflib dialog box opens.
- 4** In the Name pane, highlight the user SiteScope uses to access the remote machine. In the Permissions pane, select the **Allow** check box for **Read**. Click **OK** to save the configuration and close the Permissions for Perflib dialog box.
- 5** In the **HKEY\_LOCAL\_MACHINE** window, select **SYSTEM > CurrentControlSet > Control > SecurePipeServers > winreg**. Click **Security** in the Registry Editor tool bar and select **Permissions**. The Permissions for Winreg dialog box opens.

- 6 In the Name pane, highlight the user that SiteScope uses to access the remote machine. In the Permissions pane, select the **Allow** check box for **Read**. Click **OK** to save the configuration and close the Permissions for Perflib dialog box.
- 7 In the Registry Editor tool bar, click **Registry** and select **Exit** to save the configuration and exit.
- 8 Restart the SiteScope machine.

---

**Note:** For information about enabling non-administrative users to monitor performance on a remote machine, refer to the Microsoft Knowledge Base (<http://support.microsoft.com/kb/q164018/>).

---

#### To configure Windows 2000:

- 1 On the SiteScope machine, select **Start > Programs > Administrative Tools > Computer Management**. The Computer Management dialog box opens.
- 2 In the System Tools tree, expand the **Local Users and Groups** tree and select **Groups**. All groups on the machine are listed in the right-hand pane.
- 3 In the right-hand pane, select the **Administrators** group. The Administrators Properties dialog box opens.
- 4 If the user that SiteScope uses to access the remote machine is listed in the Members pane, go to step 5. If the user is not listed, click **Add**. The Select Users or Groups dialog box opens.
  - a Enter the user in the text box.
  - b Click **OK** to save the configuration and close the Select Users or Groups dialog box.
- 5 Click **OK** to save the configuration and close the Administrators Properties dialog box.
- 6 In the Computer Management dialog box, click **File** in the tool bar and select **Exit**.
- 7 Restart SiteScope on the SiteScope machine.

## **Configure the WMI Service for Remote Monitoring**

This task describes the steps involved in configuring SiteScope to monitor data on remote Windows servers using Windows Management Instrumentation (WMI). Using WMI, you can access system counter data from objects in the performance libraries. This is the same performance data that appears in the Perfmon utility.

This task includes the following steps:

- ▶ “Prerequisites” on page 1284
- ▶ “Configure the WMI Service on the Remote Server” on page 1284
- ▶ “Configure WMI Preference Settings in SiteScope - Optional” on page 1285
- ▶ “Configure a Monitor” on page 1285

### **1 Prerequisites**

SiteScope must be installed on a Windows machine.

### **2 Configure the WMI Service on the Remote Server**

The following are requirements for using SiteScope to collect performance measurements on a remote machine using WMI:

- ▶ The WMI service must be running on the remote machine. For details on using WMI, refer to the Windows Management Instrumentation documentation ([http://msdn.microsoft.com/en-us/library/aa826517\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa826517(VS.85).aspx)).
- ▶ The user entered on the WMI remote server must have permissions to read statistics remotely from WMI namespace **root\CIMV2**. For details on namespace security in WMI, refer to <http://support.microsoft.com/kb/295292>.

For information about troubleshooting WMI service problems, see “WMI Troubleshooting and Limitations” on page 1314.

### 3 Configure WMI Preference Settings in SiteScope - Optional

You can configure the connection type for monitoring Windows server resources on the local host machine and the WMI timeout settings in **Preferences > General Settings > WMI Preferences**. For details on the user interface, see “WMI Preferences” on page 1384.

### 4 Configure a Monitor

Add a WMI supported monitor, and configure the monitor settings. For the list of monitors that support the WMI protocol, see “Monitors Supporting Windows Management Instrumentation (WMI)” on page 343.

## Configure SiteScope to Monitor a Remote UNIX Server

This task describes the steps involved in configuring SiteScope to monitor data on remote UNIX servers.



This task includes the following steps:

- “Enable SiteScope to Monitor Data on Remote UNIX Servers” on page 1286
- “Configure and Test the Settings for the UNIX Remote Server” on page 1286
- “Results” on page 1286

## 1 Enable SiteScope to Monitor Data on Remote UNIX Servers

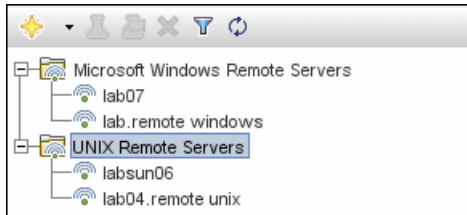
To enable SiteScope to monitor data on remote UNIX servers, define an individual remote UNIX server connection profile for each server. For details on how to perform this task, see “Define Remote UNIX Server Connection Profiles” on page 1287.

## 2 Configure and Test the Settings for the UNIX Remote Server

- a Configure the remote UNIX server in the remote server tree. For details on the user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.
- b Test the settings for the applicable server.
  - Click the **Test**  button to test the connection to the server.
  - Click the **Detailed Test**  button to test the running commands on the remote host and check the permissions for the defined user.

## 3 Results

The server is added to the list of UNIX Remote Servers in the remote server tree. You can then create monitors to watch the resources and performance counters for that server. Multiple monitors can use the same connection profile.



## Define Remote UNIX Server Connection Profiles

Monitoring remote UNIX server data requires authenticated access to the remote server. A UNIX server connection profile provides the necessary address and login credentials for SiteScope to log on to a remote server.

**To log on to a remote server using the UNIX server connection profile, either:**

- Log on to the remote server as a user with administrator privileges, or
- Create or modify a user account on the remote server that corresponds with the connection method and login permissions used in the SiteScope connection profile for that server.

## Remote Servers User Interface

**This section includes:**








- Remote Server Properties Page on page 1288
- New/Edit Microsoft Windows Remote Server Dialog Box on page 1291
- New/Edit UNIX Remote Servers Dialog Box on page 1299

 **Remote Server Properties Page**

<b>Description</b>	<p>Displays information about the remote servers configured in your network environment.</p> <p>Use this page to add, edit, or delete remote server profiles.</p> <p><b>To access:</b> Select the <b>Remote Servers</b> context. In the remote servers tree, click the <b>Microsoft Windows Remote Servers</b> or <b>UNIX Remote Servers</b> container.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit remote servers</b> permissions can view or edit the Remote Servers page.</li> <li>▶ You cannot delete a server from the list of remote servers if the server is referenced by a monitor. Select a different server in the <b>Server</b> box of the Monitor Settings panel for each monitor that references the remote server, and then delete the remote server from the remote server list.</li> <li>▶ You can create multiple remote servers for the same host machine.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277</li> <li>▶ “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Remote Servers Overview” on page 1276</li> <li>▶ “Remote Server Tree” on page 83</li> </ul>



The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click the <b>New Microsoft Windows/UNIX Remote Server</b> button to configure a remote server and add it to the tree. For details, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291 and “New/Edit UNIX Remote Servers Dialog Box” on page 1299.
	Click the <b>Edit Remote Server</b> button to edit the properties of the selected remote server.
	Click the <b>Delete Remote Server</b> button to delete the selected server from the tree.
	Click the <b>Test</b> button to test the connection to the server.
	Click the <b>Detailed Test</b> button to run a test that displays the result of running commands on UNIX remote servers. This enables checking the permissions for the defined user.
	Click the <b>Select All</b> button to select all listed remote servers.
	Click the <b>Clear Selection</b> button to clear the selection.
<Remote servers list>	Lists the remote servers that have been configured in SiteScope. Double-click a remote server to open the Edit Remote Server page for the selected remote server type. For details, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291 and “New/Edit UNIX Remote Servers Dialog Box” on page 1299.
<b>Name</b>	The name by which the remote server is known in SiteScope.
<b>Server</b>	The IP address or name of the monitored remote server. You can create two remote servers with the same host name.

GUI Element (A-Z)	Description
<b>Status</b>	The connection status of the remote server. If SiteScope is unable to connect to the remote server, a reason for the connection failure is provided.
<b>Operating System</b>	The operating system that is running on the remote server.
<b>Method</b>	The connection type for monitoring the server resources (NetBIOS, SSH, WMI, Rlogin, Telnet).
<b>Description</b>	A description of the remote server.

 **New/Edit Microsoft Windows Remote Server Dialog Box**

<b>Description</b>	<p>SiteScope on Windows can monitor systems and services running on remote Windows servers for a large number of statistics without the installation of agent software on each server. This includes monitoring server resources such as CPU, Disk Space, Memory, and Windows-specific performance counter data. Select the servers to display when configuring monitors. SiteScope creates a new remote connection profile for each server address in the list.</p> <p><b>To access:</b> Select the <b>Remote Servers</b> context.</p> <ul style="list-style-type: none"> <li>▶ To add a Microsoft Windows remote server, right-click the <b>Microsoft Windows Remote Servers</b> container, and select <b>New Microsoft Windows Remote Server</b>.</li> <li>▶ To edit an existing Microsoft Windows remote server, expand the <b>Microsoft Windows Remote Servers</b> container, and select the remote server you want to edit.</li> </ul>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit remote servers</b> permissions can view or edit the Remote Servers page.</li> <li>▶ You cannot delete a server from the list of remote servers if the server is referenced by a monitor. Select a different server in the <b>Server</b> box of the Monitor Settings panel for each monitor that references the remote server, and then delete the remote server from the remote server list.</li> </ul>
<b>Included in Tasks</b>	<p>“Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Remote Servers Overview” on page 1276</li> <li>▶ “Remote Server Tree” on page 83</li> <li>▶ “Remote Server Properties Page” on page 1288</li> <li>▶ “Troubleshooting and Limitations” on page 1309</li> </ul>

The following elements are included:

GUI Element	Description
<b>Save</b>	Saves the settings without verifying the correctness of the configuration on the remote server. <b>Note:</b> Performance is faster than if you save and test configuration settings, because SiteScope does not need to establish a connection and verify the settings on a remote server.
<b>Save &amp; Test</b>	Saves the settings and verifies the correctness of the configuration on the remote server. If SiteScope fails to connect to the remote server, or if there is an invalid property in the configuration settings, an error message is displayed. <b>Note:</b> Performance is slower than if you just save the configuration settings, because SiteScope must establish a connection and verify the settings on a remote server.


### General Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Name</b>	Enter a name by which the remote machine should be known in SiteScope. This name appears in the <b>Server</b> list of monitors that can use this connection profile. <b>Note when working in template mode:</b> <ul style="list-style-type: none"> <li>▶ For each template monitor that requires this remote server, you must enter this same value in the <b>Servers</b> box for the template monitor.</li> <li>▶ Names must be unique, otherwise the deployment fails.</li> </ul>
<b>Description</b>	Add a text description for the remote Windows server. This text appears only when editing the remote's properties.

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<p><b>Server</b></p>	<p>Enter the real IP address or UNC name of the monitored Windows server (virtual IP addresses are not supported). An IP host name also works if the SiteScope server is able to translate this common name into an IP address by using a hosts file, DNS, or WINS/DNS integration.</p> <p>You can create multiple remote servers for the same host machine. For example, you can create one remote server that uses the NetBIOS protocol and another that uses WMI for the same host machine, provided the name in General Settings is unique.</p> <p>To use the same login credentials to configure multiple servers at the same time, enter the server names or addresses separated by a comma (","), semi-colon (";"), or a space. For example: \\server1,\\server2,\\.</p> <p><b>Note:</b> In the list of Windows Remote Servers, click the <b>Test</b>  button to test connectivity after the profiles have been added.</p> <p><b>Note when working in template mode:</b> Enter the name of a template variable that represents the remote server name, for example, %%host%%. This enables you to add each server as you deploy the template when asked to enter the required information for the variables. Each time you enter a server name for the variable, a monitor instance is created for that server and the server is added to the remote server tree. If the host name does not match a server name at that time, the monitor fails.</p> <p>If the remote servers onto which you want to deploy monitor templates already exist under Remote Servers, you can reference these servers within the monitor template. You do this by referencing the system variable \$\$\$SERVER_LIST\$\$ which identifies the servers accessible to the SiteScope. For details, see “Syntax for System Variables” on page 1569.</p>

GUI Element	Description
<b>Credentials</b>	<p>Select the option for providing the user name and password for the remote Windows server.</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials.</li> <li>▶ <b>User name.</b> Enter the user name for the remote server or use a template variable that represents the user login name (for example, %%user%%).  <b>Note:</b> If the server is within the same domain as the SiteScope machine, include the domain name in front of the user login name. For example: &lt;DOMAIN&gt;\&lt;username&gt;. If using a local machine login account for machines within or outside the domain, include the machine name in front of the user login name. For example: &lt;machinename&gt;\&lt;username&gt;.</li> <li>▶ <b>Password.</b> Enter the password for the remote server or the passphrase for the SSH key file, or use a template variable that represents the password (for example, %%password%%). When using SSH authentication with public/private key based authentication enter the passphrase for the identity file here.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password for the server (selected by default). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>Trace</b>	<p>Select to trace messages to and from the subject server, recorded to the SiteScope RunMonitor.log file.</p> <p><b>Default value:</b> Not selected</p>

GUI Element	Description
<b>Method</b>	<p>SiteScope uses one of the following connection types for monitoring Windows server resources. From the drop-down list select:</p> <ul style="list-style-type: none"> <li>▶ <b>NetBIOS.</b> The default server-to-server communication protocol for Microsoft Windows NT and 2000 networks.</li> <li>▶ <b>SSH.</b> Secure Shell, a more secured communication protocol that can be installed on Microsoft Windows NT/2000 based networks. This connection method normally requires installing SSH libraries on each server to be connected. For more information see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1317.</li> <li>▶ <b>WMI.</b> Windows Management Instrumentation, a more secured communication protocol than NetBIOS, supports Windows server monitors that use perfmon to gather performance data. For the list of monitors that support WMI, see “Monitors Supporting Windows Management Instrumentation (WMI)” on page 343. For details on how to configure the WMI service for remote monitoring, see “Configure the WMI Service for Remote Monitoring” on page 1284.</li> </ul> <p><b>Note:</b> Remote servers that have been configured with the WMI method are not displayed in the list of available remote servers when configuring a monitor that does not support WMI.</p>
<b>Remote machine encoding</b>	<p>Enter the encoding for the remote server, if the remote server is running an operating system version that uses a different character encoding than the server on which SiteScope is running. This enables SiteScope to display encoded content correctly.</p> <p><b>Default value:</b> Cp1252 encoding</p>

## Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>SSH connection method</b>	<p>Select the client to use for this connection from the list. The currently supported clients are:</p> <ul style="list-style-type: none"> <li>▶ <b>Internal Java Libraries.</b> Connect using the Java SSH client integrated with SiteScope.</li> <li>▶ <b>Plink/External SSH.</b> Connect using an external SSH client. On Windows, SiteScope includes Plink.</li> </ul>
<b>SSH port number</b>	<p>Enter the port on which the remote SSH server is listening.</p> <p><b>Default value:</b> 22</p>
<b>Connection limit</b>	<p>Enter the number of open connections that SiteScope allows for this remote. If there are many monitors configured to use this connection, set the number of open connections high enough to relieve a potential bottleneck.</p> <p><b>Default value:</b> 3</p> <p><b>Note:</b> This setting does not effect running tests for a remote server. Tests always create a new connection.</p>
<b>SSH authentication method</b>	<p>Select the authentication method to use for SSH connections from the drop-down list. The currently supported methods are:</p> <ul style="list-style-type: none"> <li>▶ <b>Password.</b> Authenticate using a password.</li> <li>▶ <b>Key File.</b> Authenticate using public/private key authentication. When this option is selected SiteScope uses the private key in the file <code>&lt;SiteScope root directory&gt;\groups\identity</code> to authenticate. The corresponding public key must be listed in the <code>authorized_keys</code> file on the remote host. For information about SSH requirements, see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1317.</li> </ul>



GUI Element	Description
<b>Disable connection caching</b>	Select to turn off connection caching for this remote. By default, SiteScope caches open connections.
<b>Key file for SSH connections</b>	Enter the path and name of the file that contains the private key for this connection. The default key file is <b>&lt;SiteScope root directory&gt;\groups\identity</b> . This setting applies only when the authentication method is Key File.
<b>SSH version 2 only</b>	Select to force SiteScope to use SSH protocol version 2 only. This option applies only when using the integrated Java Client. For information about configuring an external SSH client to use SSH2 protocol, see “External SSH Client Overview” on page 1348.
<b>SSH keep alive mechanism</b>	Select to engage a keep alive mechanism for SSH version 2 sessions. This option applies only when using the integrated Java Client.
<b>SSH using preinstalled perfex</b>	Select to use a preinstalled perfex based SSH. For the list of monitors that support perfex based SSH, see “Monitors Supporting Perfex/Non-Perfex Based NT SSH” on page 1341.
<b>Custom commandline</b>	<p>Enter a custom command line for a remote server using the External Client. Use this option when passing specific commands to the external client to run. Valid substitution variable are:</p> <ul style="list-style-type: none"> <li>▶ <b>\$user\$</b>. This translates the username entered into the remote server.</li> <li>▶ <b>\$password\$</b>. This translates the password entered into the remote server.</li> <li>▶ <b>\$host\$</b>. This translates the host name entered into the remote server.</li> </ul>

## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>
<b>Add Tag</b>	<p>Click to add a new keyword tag.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>

 **New/Edit UNIX Remote Servers Dialog Box**

<b>Description</b>	<p>SiteScope can monitor systems and services running on remote UNIX servers for certain statistics (such as CPU, Disk Space, Memory, and Processes) without the installation of agent software on each server. Select the servers to display when configuring UNIX monitors. SiteScope creates a new remote connection profile for each server address in the list.</p> <p><b>To access:</b> Select the <b>Remote Servers</b> context.</p> <ul style="list-style-type: none"> <li>➤ To add a UNIX remote server, right-click the <b>UNIX Remote Servers</b> container, and select <b>New UNIX Remote Server</b>.</li> <li>➤ To edit an existing UNIX remote server, expand the <b>UNIX Remote Servers</b> container, and select the remote server you want to edit.</li> </ul>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>➤ Only an administrator in SiteScope, or a user granted <b>Edit remote servers</b> permissions can view or edit the Remote Servers page.</li> <li>➤ You cannot delete a remote server from the list of remote servers if the server is referenced by a monitor. Select a different server in the <b>Server</b> box of the Monitor Settings panel for each monitor that references the remote server, and then delete the remote server from the remote server list.</li> <li>➤ The HTTP method for connecting to a remote server is no longer supported.</li> </ul>
<b>Included in Tasks</b>	<p>“Configure SiteScope to Monitor a Remote UNIX Server” on page 1285</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Remote Servers Overview” on page 1276</li> <li>➤ “Remote Server Tree” on page 83</li> <li>➤ “Remote Server Properties Page” on page 1288</li> </ul>

The following elements are included:

GUI Element	Description
<b>Save</b>	Saves the settings without verifying the correctness of the configuration on the remote server. <b>Note:</b> Performance is faster than if you save and test configuration settings, because SiteScope does not need to establish a connection and verify the settings on a remote server.
<b>Save &amp; Test</b>	Saves the settings and verifies the correctness of the configuration on the remote server. If SiteScope fails to connect to the remote server, or if there is an invalid property in the configuration settings, an error message is displayed. <b>Note:</b> Performance is slower if than if you just save the configuration settings, because SiteScope must establish a connection and verify the settings on a remote server.



### General Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Name</b>	Enter a name by which the remote machine should be known in SiteScope. This name appears in the <b>Server</b> list of monitors that can use this connection profile.
<b>Description</b>	Add a text description for the remote UNIX server. This text appears only when editing the remote's properties.

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Main Settings</b>	
<b>Server</b>	<p>Enter the real IP address or host name of the monitored server (virtual IP addresses are not supported).</p> <p>To use the same login credentials to configure multiple servers at the same time, enter the server names or addresses separated by a comma (","), semi-colon (";"), or a space.</p> <p><b>Example:</b> If using NetBIOS to connect to other servers, enter a comma-separated string of server addresses such as: <code>serveraddress1,serveraddress2,serveraddress3</code></p> <p>When completing the other required entries on the form, SiteScope creates a new remote connection profile for each server address in the list.</p> <p><b>Note:</b> To test connectivity after the host is added, click the <b>Test</b>  button in the table listing the UNIX Servers. This tests only the connection to the server. Click the <b>Detailed Test</b>  button to run a test that displays the result of running commands on the remote host. This enables checking the permissions for the defined user.</p> <p><b>Note when working in template mode:</b> Enter the name of a template variable that represents the remote server name, for example, <code>%%host%%</code>. Each time you enter a server name for the variable, a monitor instance is created for that server and the server is added to the remote server tree.</p> <p>If the remote servers onto which you want to deploy monitor templates already exist under Remote Servers, you can reference these servers within the monitor template. You do this by referencing the system variable <code>\$\$SERVER_LIST\$\$</code> which identifies the servers accessible to the SiteScope. For details, see “Syntax for System Variables” on page 1569.</p>

GUI Element	Description
<b>Credentials</b>	<p>Select the option for providing the user name and password for the remote UNIX server.</p> <ul style="list-style-type: none"> <li>▶ <b>Use user name and password.</b> Select this option to manually enter user credentials.</li> <li>▶ <b>User name.</b> Enter the user name for the remote server or use a template variable that represents the user login name (for example, %%user%%).</li> <li>▶ <b>Password.</b> Enter the password for the remote server or the passphrase for the SSH key file, or use a template variable that represents the password (for example, %%password%%). When using SSH authentication with public/private key based authentication enter the passphrase for the identity file here.</li> <li>▶ <b>Select predefined credentials.</b> Select this option to have SiteScope automatically supply a predefined user name and password for the server (selected by default). Select the credential profile to use from the <b>Credential profile</b> drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see “Configure Credential Preferences” on page 1527.</li> </ul>
<b>Trace</b>	<p>Select to trace messages to and from the remote server in the <b>RunMonitor.log</b> file.</p> <p><b>Default value:</b> Not selected</p>
<b>Operating system</b>	<p>The operating system that is running on a remote server. This is required so that the correct information can be obtained from that server. Select an operating system from the list.</p> <p>The following operating systems are supported when defining Remote Unix servers: AIX, FreeBSD, HP-UX, HP/UX, HP/UX64-bit, Linux, MacOSX, NonStopOS, OPENSERVER, Red Hat Enterprise Linux, SCO, SGI Irix, Solaris Zones, Sun Solaris, SunOS, Tru64 5.x, and Tru64 Pre 4.x (Digital). For servers running versions of UNIX which are not included in the list, see “UNIX Operating System Adapters” on page 1363.</p>

GUI Element	Description
<b>Method</b>	<p>The currently supported methods are:</p> <ul style="list-style-type: none"> <li>▶ <b>Rlogin.</b> Log in to the remote server using the Rlogin protocol.</li> <li>▶ <b>SSH.</b> Log in to the remote server using the SSH protocol. This may require additional software and setup depending on the version of UNIX. For more information on SSH requirements, see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1317.</li> <li>▶ <b>Telnet.</b> Log in to the remote server using Telnet.</li> </ul> <p>For information about the connection methods, see “Connection Methods for Remote UNIX” on page 1308.</p>
<b>Prompt</b>	<p>This is the prompt output when the remote system is ready to handle a command.</p> <p><b>Default value:</b> #</p>
<b>Login prompt</b>	<p>This is the prompt output when the system is waiting for the login to be entered.</p> <p><b>Default value:</b> &gt;</p>
<b>Password prompt</b>	<p>This is the prompt output when the system is waiting for the password to be entered.</p> <p><b>Default value:</b> assword:</p>
<b>Secondary prompt</b>	<p>Enter the secondary prompts if the telnet connection to the remote server causes the remote server to prompt for more information about the connection. Separate multiple prompt string by commas (,).</p> <p><b>Example:</b> For Telnet connections to some remote servers, the remote server may ask what terminal type should be emulated for the connection. In this case, enter <b>Terminal type?</b> as the secondary prompt. The response to the secondary prompt is entered in the <b>Secondary Response</b> box below.</p>
<b>Mask secondary response</b>	<p>Enables you to hide the secondary response behind asterisks. If you subsequently clear the check box, the hidden data is deleted.</p> <p><b>Default value:</b> Not selected</p>

GUI Element	Description
<b>Secondary response</b>	Enter the responses to any secondary prompts required to establish connections with this remote server. Separate multiple responses with commas (,).
<b>Initialize shell environment</b>	<p>Enter any shell commands to be run at the beginning of the session. Separate multiple commands with a semicolon (;). This option specifies shell commands to be run on the remote machine directly after a Telnet or SSH session has been initiated. These commands can be used to customize the shell for each SiteScope remote. Some examples include:</p> <ul style="list-style-type: none"> <li>▶ The remote shell may not have the correct path set for SiteScope scripts to run. The following command adds the directory <code>/usr/local/bin</code> into the PATH of the current shell on the remote machine: <code>export PATH=\$PATH:/usr/local/sbin</code></li> <li>▶ The remote shell may not be initializing the pseudo terminal correctly. Enter the following command to increase the terminal width to 1024 characters: <code>stty cols 1024;\${SHELL}</code></li> </ul> <p><b>Note:</b> Commands after a shell invocation are not run.</p> <ul style="list-style-type: none"> <li>▶ There have been cases where the remote Telnet Server does not echo back the command line properly. This may cause strange behavior for monitors that rely on this behavior. Enter the following command to force the remote terminal to echo: <code>stty echo</code></li> <li>▶ Certain UNIX shells have been known to behave erratically with SiteScope. This includes bash, ksh, and csh. Enter the following command to change the shell to sh for the SiteScope connection: <code>/bin/sh</code></li> </ul>
<b>Remote machine encoding</b>	<p>Enter the encoding for the remote server if the remote server is running an operating system version that uses a different character encoding than the server on which SiteScope is running. This enables SiteScope to display encoded content correctly.</p> <p><b>Default value:</b> Cp1252 encoding</p>
<b>NonStop Shell Settings</b>	



GUI Element	Description
Shell choice prompt	(For NonStop OS only) The prompt output when the system is waiting for the shell to be selected. <b>Default value:</b> >
Shell name	(For NonStop OS only) The shell name to be executed. <b>Default value:</b> OSS

## Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
SSH connection method	Select the client to use for this connection from the list. The currently supported clients are: <ul style="list-style-type: none"> <li>▶ <b>Internal Java Libraries.</b> Connect using the Java SSH client integrated with SiteScope.</li> <li>▶ <b>Plink/External SSH.</b> Connect using an external SSH client. On Microsoft Windows, SiteScope includes Plink. On Solaris or Linux SiteScope uses an installed client such as OpenSSH.</li> </ul>
SSH port number	Enter the port on which the remote SSH server is listening. <b>Default value:</b> 22
Connection limit	Enter the number of open connections that SiteScope allows for this remote. If there are many monitors configured to use this connection, set the number of open connections high enough to relieve a potential bottleneck. <b>Default value:</b> 3 <b>Note:</b> This setting does not effect running tests for a remote server. Tests always create a new connection.

GUI Element	Description
<b>SSH authentication method</b>	<p>Select the authentication method to use for SSH connections from the list. The currently supported methods are:</p> <ul style="list-style-type: none"> <li>➤ <b>Password.</b> Authenticate using a password.</li> <li>➤ <b>Key File.</b> Authenticate using public/private key authentication. When this option is selected, SiteScope uses the private key in the file <code>&lt;SiteScope root directory&gt;\groups\identity</code> to authenticate. The corresponding public key must be listed in the <b>authorized_keys</b> file on the remote host. For information about SSH requirements, see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1317.</li> </ul>
<b>Disable connection caching</b>	<p>Select to turn off connection caching for this remote. By default, SiteScope caches open connections.</p> <p><b>Default value:</b> Not selected</p>
<b>Key file for SSH connections</b>	<p>Enter the path and name of the file that contains the private key for this connection. The default key file is <code>&lt;SiteScope root directory&gt;\groups\identity</code>. This setting applies only when the authentication method is Key File.</p>
<b>SSH version 2 only</b>	<p>Select to force SiteScope to use SSH protocol version 2 only. This option applies only when using the integrated Java Client. For information about configuring an external SSH client to use SSH2 protocol, see “External SSH Client Overview” on page 1348.</p> <p><b>Default value:</b> Not selected</p>

GUI Element	Description
<b>SSK keep alive mechanism</b>	Select to engage a keep alive mechanism for SSH version 2 sessions. This option applies only when using the integrated Java Client.  <b>Default value:</b> Not selected
<b>Custom commandline</b>	Enter a custom command line for a remote server using the External Client. Use this option when passing specific commands to the external client to be run. Valid substitution variable are: <ul style="list-style-type: none"> <li>➤ <b>\$root\$</b>. This translates the SiteScope directory.</li> <li>➤ <b>\$user\$</b>. This translates the username entered into the remote server.</li> <li>➤ <b>\$password\$</b>. This translates the password entered into the remote server.</li> <li>➤ <b>\$host\$</b>. This translates the host name entered into the remote server.</li> </ul>

### Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>&lt;Tag name and values&gt;</b>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.  For details on using tags, see “Working with Search/Filter Tags” on page 107.
<b>Add Tag</b>	Click to add a new keyword tag.  For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.

## Connection Methods for Remote UNIX

This table includes information on the methods for connecting SiteScope to remote UNIX servers.

Connection Method	Description
<b>rlogin</b>	You can set up your remote servers to require a password for rlogin, or to enable access without a password (like "rsh"). SiteScope supports either case.
<b>SSH</b>	<p>For Solaris, using the SSH access method requires that an SSH client is installed on the SiteScope machine and the SSH server installed on the servers you are monitoring. The path to the SSH client on the machine where SiteScope is running should be <code>/usr/local/bin/ssh</code> or <code>/usr/bin/ssh</code>. For information about SSH requirements, see "SiteScope Monitoring Using Secure Shell (SSH)" on page 1317.</p> <p>For Microsoft Windows NT or 2000, an SSH client is included in the package. For debugging, the Microsoft Windows SSH client can be run from the command line, replacing the values for the username, host name, and password:</p> <pre>\SiteScope\tools\plink.exe -ssh myUser@myServer.myCompany.com -pw myPassword</pre> <p>Using SSH requires that digital certificates be installed on each of the servers to which you are connecting.</p>
<b>telnet</b>	Telnet is a popular method for connecting to remote UNIX servers. You can set up your remote servers to require a password for telnet, or to enable access without a password (like "rsh"). SiteScope handles either case.

## Troubleshooting and Limitations

This section contains troubleshooting and limitations for the following issues relating to remote servers:

- ▶ “SiteScope Monitoring of Remote Windows NT and Windows 2000 Servers” on page 1309
- ▶ “Understanding Error Codes When Testing Windows Remote Servers” on page 1310
- ▶ “Microsoft Windows Event Log Access on Remote Windows Servers” on page 1311
- ▶ “Remote Windows Connections Using Perfex” on page 1312
- ▶ “WMI Troubleshooting and Limitations” on page 1314
- ▶ “Remote UNIX Servers Not Configured For an English Locale” on page 1315
- ▶ “System Encoding Used when Displaying System Resources for Remote Hosts Connected Through NETBIOS” on page 1316

### **SiteScope Monitoring of Remote Windows NT and Windows 2000 Servers**

The following is additional information relating to setting up and troubleshooting SiteScope monitoring of remote Windows NT and Windows 2000 servers.

- ▶ Connect to the remote machine using PERFMON. If a connection cannot be made using this tool, there is likely a problem involving the user access permissions granted to the SiteScope account on the remote server. SiteScope requires certain administrative permissions to be able to monitor server statistics.
- ▶ For security reasons, SiteScope may not be allowed to use the permissions of a full administrator account. SiteScope can be granted restricted monitoring access by editing certain Windows Registry Keys. For information about restricting access to the registry from a remote machine, refer to the Microsoft Knowledge Base (<http://support.microsoft.com/kb/q153183/>).

- ▶ When you need to monitor a server which is a stand-alone server or not part of a domain already visible to the SiteScope server, try entering the machine name followed by a slash and then the login name in the **Login** box. For example, loneserver\sitescope.
- ▶ Some problems have been found when trying to monitor Windows 2000 servers from SiteScope running on Windows NT4. In many cases, the problem involves incompatibility of the DLL's used by the operating system to communicate between the servers.

---

**Note:**

- ▶ For additional information on how to secure performance data in Windows 2000, Windows NT, and Windows XP, refer to the Microsoft Knowledge Base (<http://support.microsoft.com/kb/q146906/>).
  - ▶ For information about troubleshooting performance monitor counter problems for Windows 2000 and Windows NT, refer to the Microsoft Knowledge Base (<http://support.microsoft.com/kb/152513/>).
- 

## **Understanding Error Codes When Testing Windows Remote Servers**

**Problem:**

In the remote server test results, the status string does not contain descriptive error codes.

**Resolution:**

Use the net helpmsg command to help explain Windows network messages and provide problem-solving information.

Run the following command line:

```
net helpmsg <error code number>
```

For example, entering net helpmsg 53 returns "The network path was not found."

## Microsoft Windows Event Log Access on Remote Windows Servers

### Problem:

When viewing Remote Windows event logs or getting alerts relating to monitoring a remote Windows machine, the following message is displayed:

The description for Event ID ( XXXX ) in Source ( XXXX ) could not be found. It contains the following insertion string(s):  
The operation has completed successfully.

### Cause:

When you view the event log on a computer from a remote computer, if the required registry keys (and referenced files) are not present on the remote computer, SiteScope is unable to format the data; hence it displays the data in a generic format.

### Resolution:

The required registry entries and DLL files must be copied to the remote computer on which the event viewer application is being run.

### To get the remote registry entries and DLL files onto the local SiteScope machine:

- 1 Locate on the remote machine which event you are not getting properly in SiteScope by finding the entry in the Event Viewer. Write down the information for the source, event id, and description. For example:

Source: MExchangeSA, Event ID: 5008, Description: The message tracking log file C:\exchsrvr\tracking.log\20020723.log was deleted.

- 2 Open the registry setting **HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\EventLog\Application** and click the source (for example, MExchangeSA).
- 3 Click **EventMessageFile** and write down the data for where that DLL is located (for example, C:\EXCHSRVR\bin\madmsg.dll).

- 4 Locate the DLL on the remote and copy it to the SiteScope machine. You can perform the copy in one of two ways:
  - ▶ Use the **Initlog.exe** utility, in the BackOffice Resource Kit, Second Edition, to copy the required registry entries from the Exchange Server computer to the remote computer. This utility can also copy the required DLL files if you are logged on to Windows NT with an account that has Administrator privilege on the Exchange Server computer (see Microsoft Article Q184719).
  - ▶ Use FTP, mail, and so forth, to get the file to your local drive.
- 5 SiteScope uses the data from the **EventMessageFile** field in step 3 to determine where to find the DLL on the local machine. You must create the same folder structure as in this step and place the file in that directory. Alternatively, you can change the directory structure to say `c:\Windows\System32` (SiteScope looks in the ADMIN\$ by default on the remote machine), and place the DLL in that folder, but you must have this structure and the DLL on both machines. If you do this, you must update the registry in step 3 to reflect the directory in which the DLL is located.

### **Remote Windows Connections Using Perfix**

Use the following steps to view that data is being returned when SiteScope is trying to access the remote registry:

- 1 Open a command window on the SiteScope server.
- 2 Change the directory to `<SiteScope root directory>\tools`.
- 3 Enter the following in a command line:

```
perfix \\MACHINE -u username -p password -d -elast "Application"
```

This command gives you the number of entries in your Application log. For example:

```
Connected to \\ex-srv as int-ss Next Record: 2369
```



- 4** You should list only the last 10 or 12 events to find the one you are looking for. For this example, the command is:

```
perfex \\MACHINE -u username -p password -d -elog "Application" 2355 | more
```

- 5** Look through each entry until you find the one you need. Note the Record id for easier searching next time when using the command in Step 3.
- 6** This output tells you what data SiteScope is receiving. In the example given, the following is an example of the data that typically would be returned:

```
Type: Information
Time: 02:00:24 08/01/102
Source: MSExchangeMTA
ID: 298
Category: 1
Record: 2342
Machine: EX-SRV
FILE=C:\EXCHSRVR\res\mtamsg.dll
REMOTE FILE=
String 835050d is: MTA
Next String 835054d is: OPERATOR
Next String 83505dd is: 34
Next String 835060d is: 0
Next String 835062d is:
File: C:\EXCHSRVR\res\mtamsg.dll
Remote Path:
calling FormatMessage()
Formatted Message 142 bytes long
Raw message is: The most current routing information has been loaded by the MTA,
and a text copy was saved in the fileGWART0.MTA. [MTA OPERATOR 34 0] (12)
Message: The most current routing information has been loaded by the MTA, and a text
copy was saved in the file GWART0.MTA.[MTA OPERATOR 34 0] (12)
```

The file path is where the remote file is being found. If you copy the DLL to the WINDOWS\SYSTEM, the file and remote file path like this:

```
Type: Information
Time: 03:15:00 08/01/102
Source: MSEXCHANGES Public
ID: 1221
Category: 6
Record: 2350
Machine: EX-SRV
FILE=C:\WINNT\SYSTEM32\mdbmsg.dll
REMOTE FILE=\\ex-srv\ADMIN$\SYSTEM32\mdbmsg.dll
String 835054d is: 0
Next String 835056d is:
File: C:\WINNT\SYSTEM32\mdbmsg.dll
Remote Path: \\ex-srv\ADMIN$\SYSTEM32\mdbmsg.dll
LOADING LIB REMOTE: \\ex-srv\ADMIN$\SYSTEM32\mdbmsg.dllcalling
FormatMessage()Formatted Message 89 bytes long
Raw message is: The database has 0 megabytes of free spaceafter online
defragmentation has terminated.Message: The database has 0 megabytes of free
space afteronline defragmentation has terminated.
```

## **WMI Troubleshooting and Limitations**

This section contains troubleshooting and limitations for the following WMI issues:

- ▶ “WMI Limitations” on page 1314
- ▶ “WMI Data Not Synchronized” on page 1314
- ▶ “WMI Fails to Retrieve Counters” on page 1315

### **WMI Limitations**

- ▶ It is not recommended to have more than 4000 monitors using WMI.
- ▶ The WMI implementation in SiteScope is supported for machines with an English locale only (both monitored machines and SiteScope server machine).

### **WMI Data Not Synchronized**

WMI data relies on being synchronized with the Perfmon utility. If WMI data is not synchronized, you should perform the following:

- 1 Check that the WMI service is started on the target machine. For details, refer to [http://msdn.microsoft.com/en-us/library/aa826517\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa826517(VS.85).aspx).
- 2 Check that the namespace `root\CIMV2` is configured to allow remote access to the user specified in the SiteScope WMI remote server. For details, refer to <http://support.microsoft.com/kb/295292>.
- 3 On the target machine, run the command `perfmon` and verify that the required perfmon objects appear. For details, refer to [http://msdn.microsoft.com/en-us/library/aa645516\(VS.71\).aspx](http://msdn.microsoft.com/en-us/library/aa645516(VS.71).aspx).

For details on how to rebuild these libraries, refer to <http://support.microsoft.com/?kbid=300956>.

- 4 On the target machine, run the command `perfmon /wmi` and verify that the required perfmon objects appear. For details, refer to [http://msdn.microsoft.com/en-us/library/aa645516\(VS.71\).aspx](http://msdn.microsoft.com/en-us/library/aa645516(VS.71).aspx).

If the required perfmon objects do not appear, run the command `perfmon wmiadap /f`. For details, refer to [http://msdn.microsoft.com/en-us/library/aa394528\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa394528(VS.85).aspx).

### WMI Fails to Retrieve Counters

In some cases, WMI shows n/a for counters while perfmon gives the value 0 for the same counters. This is the behavior for counters that are also not selectable using the perfmon utility. The reason that perfex is able to get values for these counters is because it bypasses perfmon and accesses them via the registry.



### Remote UNIX Servers Not Configured For an English Locale

#### Problem:

The File Monitor and Directory Monitor may fail when using UNIX remote servers that are not configured by default for an English locale or language.

#### Resolution:

Add "LANG=C; export LANG" to the **Initialize shell environment** property of the problematic UNIX remote server.

## **System Encoding Used when Displaying System Resources for Remote Hosts Connected Through NETBIOS**

This limitation affects all server monitors that use encoding of the remote host to display received data.

SiteScope uses default system encoding when displaying system resources information for the remote hosts connected through NETBIOS. The **Remote machine encoding** field (available in the remote server's "Main Settings" on page 1293) is not used. For example, if system encoding is ASCII and remote encoding is Unicode, the ASCII characters are displayed correctly and the Unicode symbols are not supported.

## SiteScope Monitoring Using Secure Shell (SSH)

SiteScope supports a number of security capabilities. One of these is support for remote server monitoring using Secure Shell (SSH) connections. You can use SSH to connect to a server and automatically send a command, so that the server runs that command and then disconnects. This is useful for creating automated processing and scripting.

### **This chapter includes:**

#### **Concepts**

- SiteScope and SSH Overview on page 1318
- Monitoring Remote Windows Servers Using SSH on page 1322

#### **Tasks**

- Configure Remote UNIX Servers for SSH monitoring on page 1324
- Configure Remote Windows Servers for SSH monitoring on page 1325

#### **Reference**

- SSH Configuration Requirements For UNIX Remote Servers on page 1340
- Monitors Supporting Perfex/Non-Perfex Based NT SSH on page 1341

**Troubleshooting and Limitations** on page 1343

## SiteScope and SSH Overview

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely accessing a remote computer. It is widely used by network administrators to remotely control Web and other kinds of servers. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by encryption. Secure Shell client machines make requests of SSH daemons or servers on remote machines.

Monitoring with SiteScope over SSH has the following basic requirements:

- 1** The servers that you want to have monitored by SiteScope using SSH must have a SSH daemon (or server) installed and active.
- 2** There are two SSH client options for use on the server or machine on which SiteScope is running (it is recommended to use the internal Java libraries):
  - ▶ SiteScope includes a SSH client written in Java and native to the SiteScope application code. This client eases the setup of SSH connections and generally uses fewer system resources than external SSH clients.
  - ▶ SiteScope on Windows includes a third-party SSH client called plink. Plink is part of a set of SSH tools called PuTTY. SiteScope on UNIX and Linux require that an external SSH be installed on the machine where SiteScope is running.

This section includes the following topics:

- ▶ “SSH Connectivity Options” on page 1319
- ▶ “Guidelines” on page 1321

## SSH Connectivity Options

The following tables outline the SSH connectivity options currently supported with SiteScope. For important information about configuring and managing SSH connectivity, see “Guidelines” on page 1321.

### SiteScope Installed on Windows Platform:

Target	SiteScope Client Options	Relevant Target Servers	Comments
Windows	<ul style="list-style-type: none"> <li>▶ SiteScope integrated Java SSH Client</li> <li>▶ PuTTY SSH client (included with SiteScope)</li> </ul>	SSH server (Cygwin OpenSSH or F-Secure)	<ul style="list-style-type: none"> <li>▶ Non-perfex based SSH. The RemoteNTSSH package is not required for monitors that support non-perfex based SSH. For a list of non perfex-based SSH supported monitors, see “Monitors Supporting Perfex/Non-Perfex Based NT SSH” on page 1341.</li> <li>▶ Perfex based SSH. The RemoteNTSSH package should be installed under the home user directory on the remote server. For details, see “Install SiteScope Remote NT SSH Files” on page 1337.</li> </ul>
UNIX/ Linux	<ul style="list-style-type: none"> <li>▶ SiteScope integrated Java SSH Client</li> <li>▶ PuTTY SSH client (included with SiteScope)</li> </ul>	SSH host daemon ( <code>sshd</code> - either proprietary or OpenSSH)	

**SiteScope Installed on UNIX or Linux Platform:**

Target	SiteScope Client Options	Relevant Target Servers	Comments
Windows	<ul style="list-style-type: none"> <li>▶ SiteScope integrated Java SSH Client</li> <li>▶ SSH client (/usr/local/bin/ssh or usr/bin/ssh)</li> </ul>	SSH server (Cygwin OpenSSH or F-Secure)	<p>Enable Windows monitoring from a UNIX installed SiteScope using SSH by selecting <b>Allow Unix to NT in Preferences &gt; Infrastructure Preferences &gt; General Settings</b>.</p> <ul style="list-style-type: none"> <li>▶ Non-perfex based SSH. The RemoteNTSSH package is not required for monitors that support non-perfex based SSH. For a list of non perfex-based SSH supported monitors, see “Monitors Supporting Perfex/Non-Perfex Based NT SSH” on page 1341.</li> <li>▶ Perfex based SSH. The RemoteNTSSH package should be installed under the home user directory on the remote server. For details, see “Install SiteScope Remote NT SSH Files” on page 1337.</li> </ul>
UNIX/ Linux	<ul style="list-style-type: none"> <li>▶ SiteScope integrated Java SSH Client</li> <li>▶ SSH client (/usr/local/bin/ssh or usr/bin/ssh)</li> </ul>	SSH host daemon ( <b>sshd</b> - either proprietary or OpenSSH)	



## Guidelines

- ▶ There are two different versions of the SSH protocol: version 1 and version 2. Version 1 and version 2 are different protocols and are not compatible with each other. This means that the SSH clients and SSH hosts must be configured to use the same protocol version between them to communicate. In many cases, SSH version 1 (SSH1) is the default version used. Some security vulnerabilities have been found in SSH version 1. Also, the SSH1 protocol is not being developed anymore and SSH2 is considered the current standard. We recommend using SSH version 2 (SSH2) for all SSH connections.
- ▶ The release version number of the SSH utilities and libraries you have installed must not be confused with the version of the SSH protocol that you want to be using. For example, OpenSSH release 3.5 supports both SSH1 and SSH2 protocols. The release version 3.5 does not mean that the libraries use an SSH version 3.5 protocol. You must configure the OpenSSH software to use either SSH1 or SSH2.
- ▶ If you have set up SiteScope remote monitoring using SSH connections and then make configuration changes or upgrades to the SSH daemon or server software deployed on remote servers in the environment, it may be necessary to reconfigure the SSH connectivity between the machine on which SiteScope is running and the remote servers that are being monitored.
- ▶ The availability of the Integrated Java SSH Client is indicated by using the drop-down menu in the **SSH connection method** of the Advanced Settings section of the UNIX Remote Servers and Microsoft Windows Remote Servers page. If the option for Internal Java Libraries does not appear in the list, you can still use the Plink external SSH Client for SSH connections. You can also contact an HP sales representative to upgrade to a later version of SiteScope that includes the Integrated Java SSH Client.

## Monitoring Remote Windows Servers Using SSH

The default remote connection method used by SiteScope for Windows-to-Windows connectivity and monitoring in Windows NT/2000/2003 networks is NetBIOS. While this has provided ease of connectivity, it does have several disadvantages. One is that NetBIOS is relatively vulnerable in terms of network security. Another is that it does not support remote execution scripts. Running commands on remote servers requires that scripts be run locally with commands to the remote machine being written using the UNC syntax of remote servers. Even then, some parameters are not returned from the remote server by using NetBIOS.

---

**Note:** SiteScope also supports the Windows Management Instrumentation (WMI) protocol which is a more secured communication protocol than NetBIOS for gathering data from remote servers running on Windows servers. For details on configuring the WMI service on the remote machine, see “Configure the WMI Service for Remote Monitoring” on page 1284.

---

SiteScope supports monitoring of remote Windows NT/2000 servers using SSH. This technology has been tested with the OpenSSH binaries from Cygwin (available at <http://www.cygwin.com/>) installed as the SSH server on the remote server. It has also been tested with the server available from F-Secure. You can also try OpenSSH for Windows (formerly Network Simplicity "OpenSSH on Windows") which is available on SourceForge (available at <http://sshwindows.sourceforge.net/>).

The following is a comparison overview of two of the packages.

OpenSSH Package	Advantages	Disadvantage
Cygwin OpenSSH	<ol style="list-style-type: none"> <li>1. Provides access to either Windows or UNIX-style scripting on a Windows machine.</li> <li>2. Provides access to UNIX-style system tools and utilities.</li> <li>3. SiteScope can access the remote server both as a Windows Remote and /or a UNIX Remote.</li> </ol>	Complicated setup procedure.
OpenSSH for Windows	Simple setup procedure.	Only provides access to Windows commands, scripts, and utilities.

---

**Note:**

- OpenSSH for Windows and the Cygwin SSH implementations are incompatible with each other. They should not be installed on the same machine.
  - If there is more than one version of the Cygwin utilities or more than one SSH server installed on a machine, there may be conflicts that prevent the SSH connections from working. An error message such as could not find entry point is one indication of this kind of conflict. If you suspect this error, search the machine for multiple copies of cygwin1.dll. It may be necessary to remove all versions of the utilities and then reinstall only a single installation to resolve this problem.
- 

For details on configuring remote Windows servers for SSH monitoring, see “Configure Remote Windows Servers for SSH monitoring” on page 1325.

## **Configure Remote UNIX Servers for SSH monitoring**

SiteScope for Solaris or Linux supports remote monitoring by using SSH. This task describes the steps involved in configuring remote UNIX Servers for SSH monitoring with SiteScope.

---

**Note:** Setting up the SSH hosts on the remote servers you want to monitor in the UNIX environment can be very complex and is beyond the scope of this document. Some suggested resources on installation of the OpenSSH daemon are <http://www.sunfreeware.com/openssh.html> (for Solaris) and <http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/ref-guide/s1-ssh-configfiles.html> (for Redhat Linux).

---

This task includes the following steps:

- ▶ “Prerequisites” on page 1324
- ▶ “Configure the SSH Client to Connect to the Remote Servers” on page 1324
- ▶ “Configure UNIX Remote Settings to Use the SSH Connection Method” on page 1325

### **1 Prerequisites**

For details on the requirements for configuring remote UNIX servers for SSH monitoring with SiteScope in a UNIX environment, see “SSH Configuration Requirements For UNIX Remote Servers” on page 1340.

### **2 Configure the SSH Client to Connect to the Remote Servers**

After you have set up SSH servers or daemons on remote servers, you must configure the SSH client that SiteScope uses to connect to the remote servers.

For details on how to perform this task, see “SiteScope SSH Client Connection Options” on page 1339.

### **3 Configure UNIX Remote Settings to Use the SSH Connection Method**

Once you have confirmed SSH connectivity, create or configure UNIX Remote settings in SiteScope to use SSH as the connection method.

For details on the user interface, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.

## **Configure Remote Windows Servers for SSH monitoring**

This task describes the steps involved in configuring remote Windows Servers for SSH monitoring with SiteScope.

This task includes the following steps:

- “Install and Configure a SSH Server” on page 1326
- “Enable NT SSH Monitoring Using Perfex - Optional” on page 1326
- “Install SiteScope Remote NT SSH Files” on page 1327
- “Configure the SSH Client to Connect to the Remote Servers” on page 1327
- “Configure Windows Remote Settings to Use the SSH Connection Method” on page 1327

## 1 Install and Configure a SSH Server

Install and configure a SSH server on each remote server to which you want SiteScope to connect. There are two software packages generally available that enable SSH capability:

- ▶ Cygwin environment available from RedHat at <http://www.cygwin.com/>. For details on how to perform this task, see “Install Cygwin OpenSSH on Windows” on page 1328.
- ▶ OpenSSH for Windows available at OpenSSH for Windows. For details on how to perform this task, see “Install OpenSSH for Windows” on page 1335.

---

**Note:** These setup steps must be performed for each server that runs the SSH daemon or server.

---

## 2 Enable NT SSH Monitoring Using Perfex - Optional

Depending on the monitor that you are using, you can choose to use perfex based or non-perfex based NT SSH for monitoring the remote server. By default, remote servers are monitored using non-perfex based NT SSH. For the list of monitors that support perfex based and non-perfex based NT SSH, see “Monitors Supporting Perfex/Non-Perfex Based NT SSH” on page 1341.

- ▶ **Perfex based NT SSH.** To enable SSH monitoring of the remote server using the preinstalled perfex, select the remote server in the remote servers tree, and select **SSH using preinstalled perfex** in the Advanced Settings panel.
- ▶ **Non-perfex based NT SSH.** If a monitor supports both perfex based and non-perfex based NT SSH, we recommend using non-perfex based NT SSH. To monitor using non-perfex based NT SSH, make sure that the **SSH using preinstalled perfex** check box is cleared in the Advanced Settings panel. If you are using non-perfex based NT SSH, you do not need to install SiteScope remote NT SSH files on the remote Windows server.

### **3 Install SiteScope Remote NT SSH Files**

---

**Note:** SiteScope remote NT files do not need to be installed on remote Windows server monitors that support non-perfex based SSH. For a list of monitors that support non-perfex based SSH, see “Monitors Supporting Perfex/Non-Perfex Based NT SSH” on page 1341.

---

Install the SiteScope remote SSH files on each remote Windows server to enable commonly used server monitoring functions.

For details on how to perform this task, see “Install SiteScope Remote NT SSH Files” on page 1337.

### **4 Configure the SSH Client to Connect to the Remote Servers**

After you have set up SSH servers or daemons on remote servers, you must configure the SSH client that SiteScope uses to connect to the remote servers.

For details on how to perform this task, see “SiteScope SSH Client Connection Options” on page 1339.

### **5 Configure Windows Remote Settings to Use the SSH Connection Method**

After confirming SSH connectivity between SiteScope and the remote server, you can set up Windows Remote settings in SiteScope to use SSH as the connection method. You can then configure CPU, Disk, Memory, Microsoft Windows Performance Counter, and Script monitors to use the SSH connectivity.

For details on selecting SSH as the connection method in the user interface, in “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.

## Install Cygwin OpenSSH on Windows

This task describes the steps involved in installing and configuring a Cygwin OpenSSH server on Windows servers.

---

**Important:** The following instructions assume that no other Cygwin or other ssh utilities are installed on the machine and that the machine has Internet access.

---

**Note:** The user login account used to install and run the SSH daemon needs adequate permissions to install the necessary programs, configure several file options, and control Windows services. It does not need to be the account that SiteScope uses to connect to the subject server, although that account must be configured within the Cygwin installation before you can monitor that server with SiteScope.

---

### To install and configure a Cygwin OpenSSH server on Windows NT/2000 servers:

- 1 Create a new System Environment variable with the following definition:  
CYGWIN = ntsec tty.
- 2 Add the string ;C:\cygwin\bin to your PATH variable. Save the changes to the variables.
- 3 Download the Cygwin setup program into a temporary folder. For example: C:\temp. The setup program is used to select, download, and install different packages and components available with Cygwin.
- 4 Run the downloaded setup program and choose the **Install from Internet** option when prompted to Choose A Download Source. Click **Next** to continue.
- 5 If prompted, select a root install directory where the Cygwin package should be installed. This is where the SSH daemon and related files are installed. For example, C:\cygwin. Click **Next** to continue.



- 6 If prompted, select a temporary directory where the Cygwin installation files should be stored. For example, C:\temp. Click **Next** to continue.
- 7 If prompted, select an Internet Connection option. Normally, **Direct Connection** can be used. Click **Next** to continue.
- 8 Select a suitable mirror site from which to retrieve the files using the selection list when prompted. Click **Next** to continue.
- 9 The Setup program queries the mirror site for the packages available and displays a hierarchy tree of package categories. To view and select the packages to download, click on the plus (+) symbol to the left of the category name to expand any of the package trees. Packages that are selected for download and installation display a version number in the **New** column. If a version number is not displayed for a particular package, it is not downloaded and installed. Click **Skip** to the left of package name to select the package for download.

---

**Note:** Many of the development (Devel) and database (Database) tools that may be selected by default for download are not necessary to run the SSH daemon and can be deselected to reduce download time and installation space.

---

Select each of the following packages for download and installation:

- cygrunsrv from the Admin branch
- cygwin-doc from the Doc branch
- pdksh from the Shells branch
- openssh and openssl from the Net branch
- your choice of UNIX-style text editor from the Editors branch (for example: vim or emacs)

Then click to download the files as prompted.

- 10 Depending on your installation options, the Cygwin setup downloads and installs the selected packages. You may be prompted to choose to have a shortcut to the Cygwin terminal window added to the Desktop or Program Start menu. Click to continue and complete the installation.

- 11 After the Cygwin setup is complete, open a Cygwin terminal window by clicking on the **Cygwin** desktop shortcut or Program Start menu item.

---

**Note:** Depending on the user profile in the Windows system, the default directory that opens in the terminal window may not be within the root Cygwin installation tree. Use the `pwd` command to display the current directory. Typing in the command string `cd /` normally changes the directory to the Cygwin root, which by default corresponds to the Windows `C:\cygwin` directory.

---

Update the default Cygwin group file with the group names in use on the machine and on your network. Use the `mkgroup` utility to update the default Cygwin group file with the groups defined on the server and in your domain. Examples of the commands to use are as follows:

```
mkgroup -l >> ../etc/group
mkgroup -d >> ../etc/group
```

---

**Note:**

- To have Cygwin recognize both domain and local group accounts, run the `mkgroup` utility twice, once for local users (`-l` option) and once for domain users (`-d` option). Remember to use `>>` syntax and not just `>`, to append entries to the file.
  - If you use both the local and domain options, you must manually edit the `/etc/group` file (using the UNIX style text editor you downloaded) to remove any duplicate group entries. You may also want to remove group entries that are not needed for monitoring or should not have access to this machine.
-

Update the default Cygwin user (`passwd`) file with the users defined on the local machine plus any individual domain users you want to grant access to Cygwin on this machine. Use the `mkpasswd` utility to update the default Cygwin user file.

Examples of the commands to use are as follows:

```
mkpasswd -l >> ..\etc\passwd  
mkpasswd -d -u username >> ..\etc\passwd (domain users)
```

---

**Note:**

- ▶ By default, Cygwin is set to run the OpenSSH daemon as the local user called `SYSTEM`. To have Cygwin recognize both domain and local machine user accounts, run the `mkpasswd` using the `-l` option to add all local users, and run it with the `-d` and `-u` options to add individual domain users. Remember to use `>>` syntax and not just `>`, to append entries to the file.
- ▶ If you use both the local and domain options, you must manually edit the `/etc/passwd` file (using the UNIX style text editor you downloaded) to remove any duplicate user entries. You may also change the default `/home` path and default shell for individual users. This may be necessary to install the `RemoteNTSSH` package in the `/home/sitescopeaccount/` directory of the user account to be used by SiteScope.

- 
- 12** Change the active directory to the `/bin` directory by typing `cd /bin`.
  - 13** Create a symbolic link in the `/bin` directory that points to the Windows Command (CMD) shell by entering the following command line (be sure to include the trailing space and period):

```
ln -s /cygdrive/c/winnt/system32/cmd.exe .
```

- 14** We recommend that you change permissions and ownership of several Cygwin files and directories. Also create a log file for the SSH daemon. Enter the following command lines in the Cygwin terminal command line and press ENTER after each command line entered:

```
cd /  
chmod -R og-w .  
chmod og+w /tmp  
touch /var/log/sshd.log
```

---

**Note:**

- ▶ Exact syntax is required, including spaces.
  - ▶ Inconsistent and incorrectly assigned file and directory permissions can be one reason that the SSH daemon can not be started or that SiteScope is unable to connect to and run commands or scripts on the remote server.
- 

- 15** Configure the SSH daemon to run as a Windows service by entering the following command:

```
ssh-host-config -y
```

When presented with the CYGWIN= prompt, type ntsec tty to match the environment variable you set at the beginning of this procedure. Normally, this configures the SSH daemon or service to restart automatically if the server needs to be restarted.

- 16** Configure the encryption keys and files for the SSH daemon using the following command:

```
ssh-user-config -y.
```

Enter required passphrases for several keystore files when prompted. The program asks you to re-enter the passphrase for confirmation.

- 17** You must change the ownership of several files and folders for use by the SSH daemon. The program does not normally run if the permissions on these files enable them to be changed or run by group or "world" level users. Enter the following command strings to restrict access to these files:

```
chown SYSTEM:Users /var/log/sshd.log /var/empty /etc/ssh_h*
chmod 755 /var/empty
```

- 18** Check the installation by starting and then stopping the CYGWIN sshd service using the **Programs -> Administrative Tools -> Services** panel.

---

**Note:** Cygwin includes a server utility to start the SSH daemon. However, there have been a number of situations where this method failed to start the server, whereas using the Windows Services panel was able to start the server.

---

- 19** Configure the default shell or command environment for the user account you use for monitoring with SiteScope. The shell you select effects what types of scripts or commands can be run remotely using the SSH connection. Use the UNIX-style text editor and edit the `/etc/passwd` file. Find the entry for the SiteScope login account you intend to use and change the shell from `/bin/bash` to the shell you want to use as described below. This is normally the last entry in the line for that account entry.
- a** If you chose to have SiteScope interact with the remote server using the Windows Command shell, change the default shell entry to `/bin/cmd`. Use this option when you plan to use Windows-style batch files and scripts. You must also include the symbolic link to the Windows `cmd.exe` kernel in the `/bin` directory as described in a previous step of this procedure.
  - b** If you chose to have SiteScope interact with the remote Windows server using a Cygwin UNIX shell, change the default shell entry to be `/bin/pdksh`. The SiteScope SSH client may not accurately parse Cygwin's default bash shell. You must also configure a Remote UNIX server connection to this (Windows) server that connects to the Cygwin SSH daemon.

Save the changes to the file.

- 20** Edit the PATH and the default prompt commands in the `/etc/profile` file to make sure that Cygwin can find certain files and that SiteScope can parse the output from the remote shell. Use the UNIX-style text editor and edit the `/etc/profile` file. Find the PATH definition entry near the top of the file. For example:

```
PATH=/usr/local/bin:/usr/bin:/bin:$PATH
```

Change this to include the following:

```
PATH=./usr/local/bin:/usr/bin:/bin:$PATH
```

- 21** To change the default prompt commands, edit the `/etc/profile` file, and find the section similar to the following:

```
::  
sh | -sh | */sh \  
sh.exe | -sh.exe | */sh.exe )  
#Set a simple prompt  
PS1='$ '  
::  
::
```

Immediately under this entry, add the following:

```
::  
pdksh | -pdksh | */pdksh \  
pdksh.exe | -pdksh.exe | */pdksh.exe )  
#Set a simple prompt  
PS1='> '  
::  
::
```

- 22** Save the changes to the file.
- 23** Change the active directory to the home directory of the user you have created for SiteScope monitoring.

After making these changes and starting the SSH daemon, you should be able to connect to the server using an SSH client. For information about testing SSH connectivity outside of the SiteScope application on Windows NT/2000 machines, see the section on “Testing SSH Connectivity with PuTTY Utilities” on page 1350.

---

**Note:** Any time you run the `mkpasswd -l /etc/passwd` command (for example, when adding a new user), edit the `/etc/passwd` file again to make sure that the default shell for that user is set to the required value for any account being used by SiteScope.

---

## Install OpenSSH for Windows

This task describes the steps involved in installing and configuring an OpenSSH server on Windows servers.

The OpenSSH for Windows package is an alternative to the Cygwin SSH package and can be easier to install. Like most products, the Cygwin product and the Open SSH for Windows are subject to change. There are cases where some versions of the Cygwin SSH server have not returned the data needed for SiteScope monitoring. If the OpenSSH for Windows package can solve this problem, you should use this package in place of the Cygwin package.

**To install and configure an OpenSSH for Windows server on Windows NT/2000 servers:**

- 1** Download and install the OpenSSH for Windows package.
- 2** Open a command prompt and change to the installation directory (C:\Program Files\OpenSSH is the default installation path).
- 3** Change the active directory to the OpenSSH\bin directory.
- 4** You must update the default group file with the group names in use on the machine and in your network. Use the `mkgroup` utility to update the default OpenSSH group file with the groups defined on the server and in your domain. Examples of the commands to use are as follows:

```
mkgroup -l >> ..\etc\group
mkgroup -d >> ..\etc\group
```

**Note:**

- ▶ To have OpenSSH recognize both domain and local group accounts, run the **mkgroup** utility twice, once for local users (-l option) and once for domain users (-d option). Remember to use >> syntax and not just >, to append entries to the file.
  - ▶ If you use both the local and domain options, you must manually edit the `/etc/group` file (using the UNIX style text editor you downloaded) to remove any duplicate group entries. You may also want to remove group entries that are not needed or should not have access to this machine.
- 

- 5 You must update the default OpenSSH user (`passwd`) file with the users defined on the local machine plus any domain user you want to grant access to the SSH server on this machine. Use the **mkpasswd** utility to update the default user file. Examples of the commands to use are as follows:

```
mkpasswd -l >> ..\etc\passwd
mkpasswd -d -u username >> ..\etc\passwd
```

---

**Note:**

- ▶ To have OpenSSH recognize both domain and local machine user accounts, run the **mkpasswd** utility using the -l option to add all local users and run it with the -d and -u options to add individual domain users. Remember to use >> syntax and not just >, to append entries to the file.
  - ▶ If you use both the local and domain options, you must manually edit the `/etc/passwd` file (using the UNIX style text editor you downloaded) to remove any duplicate user entries. You may also change the default `/home` path and shell for individual users (see instructions below).
- 

- 6 Check the installation by starting the **OpenSSH Server** service using the **Programs > Administrative Tools > Services** panel.



## Install SiteScope Remote NT SSH Files

This task describes the steps involved in installing SiteScope remote NT files on each remote Windows server according to the SSH package you are working with.

---

**Note:** SiteScope remote NT files do not need to be installed on remote Windows server monitors that support non-perfex based SSH. For a list of monitors that support non-perfex based SSH, see “Monitors Supporting Perfex/Non-Perfex Based NT SSH” on page 1341.

---

### To install the SiteScope SSH Files on Cygwin installations:

- 1** Verify that a `\sitescope_login_account_name` directory exists within the `<install_drive>:\cygwin\home` directory on each machine that is monitored by SiteScope using SSH. Replace `sitescope_login_account_name` with the user account name you use to connect to the machine using the SSH server.
- 2** One of the advantages of using SSH on Windows is that it allows SiteScope to run scripts on the remote server running the SSH daemon. To be able to use the Script Monitor to run remote scripts, create a `scripts` subdirectory in the `/home/sitescope_login_account_name` directory. Scripts you create for execution by the SiteScope Script Monitor must be placed inside this directory.
- 3** On the machine where SiteScope is installed, find the file called `RemoteNTSSH.zip` in the `<SiteScope root directory>\tools` directory.
- 4** Copy this file to the `<install_drive>:\cygwin\home\sitescope_login_account_name` directory on each of the remote Windows NT/2000 servers where you have installed the SSH server or daemon software.

- 5 Unzip the **RemoteNTSSH.zip** file on the remote server. Place the contents of the zip file into the `<install_drive>:\cygwin\home\sitescope_login_account_name` directory. This should create a `<install_drive>:\cygwin\home\sitescope_login_account_name\scripts` subfolder. You use this subfolder to hold scripts that can be run by the SiteScope Script Monitor.
- 6 Start the CYGWIN sshd service on the remote server.  
After you have completed the steps above, we recommend that you test SSH connectivity from your SiteScope server by using **plink.exe** or **PuTTY.exe** as described in the “Testing SSH Connectivity with PuTTY Utilities” on page 1350.

**To install the SiteScope SSH Files on OpenSSH for Windows installations:**

- 1 On the machine where SiteScope is installed, find the file called **RemoteNTSSH.zip** in the `<SiteScope root directory>\tools` directory.
- 2 Copy this file to the user home directory where the user is automatically directed after logging on to the machine via the SSH server that was previously installed. This is the directory on each of the remote Windows NT/2000 servers where you have installed the SSH server or daemon software.
- 3 Unzip the **RemoteNTSSH.zip** file on the remote server into the user home directory. This should create a `<user home directory>\scripts` subfolder. You use this subfolder to hold scripts that can be run by the SiteScope Script Monitor.
- 4 Start the OpenSSH server service on the remote server.  
After you have completed the steps above, we recommend that you test SSH connectivity from your SiteScope server by using **plink.exe** or **PuTTY.exe** as described in the “Testing SSH Connectivity with PuTTY Utilities” on page 1350.

## **SiteScope SSH Client Connection Options**

After setting up SSH servers or daemons on remote servers, configure the SSH client that SiteScope uses to connect to the remote servers using one of the following options:

- ▶ **Configure SiteScope to use the integrated Java SSH client.** SiteScope includes an integrated SSH client written in Java. This is the recommended option for SSH connectivity because it uses fewer system resources than the external clients and configuration is usually simpler.

For details on how to configure remote servers using an external client, see “Integrated Java SSH Client Overview” on page 1346.

- ▶ **Configure SiteScope to use an external SSH client.** SiteScope on Windows includes a third-party SSH client called plink. SiteScope for Solaris and Redhat Linux make use of the SSH utilities normally bundled with those operating systems or available for download.

For details on how to configure remote servers using an external client, see “External SSH Client Overview” on page 1348.

## SSH Configuration Requirements For UNIX Remote Servers

The following are requirements for configuring remote UNIX servers for SSH monitoring with SiteScope in a UNIX environment:

- ▶ Secure Shell daemons or servers (sshd) must be installed on each remote server you want to monitor with SiteScope.
- ▶ The SSH daemons on the remote servers must be running and the applicable communication ports must be open. For example, the default for SSH is port number 22.
- ▶ A SSH client must be installed on the server where SiteScope is running. The SiteScope integrated Java SSH client normally fills this requirement.
- ▶ If you use an external SSH client on Solaris or Linux, the SSH client binaries must be accessible to SiteScope. When SiteScope runs the SSH client process, it searches in both `/usr/bin` and `/usr/local/bin` for the `ssh` command. The `ssh` binaries must be in one of these two locations and SiteScope must have permissions to run the `ssh` command.

You should verify SSH client-to-server connectivity from the machine where SiteScope is running to the remote machine you want to monitor. You should check SSH connectivity outside of the SiteScope application before setting up remote server connections using SSH in SiteScope. For example, if SiteScope is running on Solaris or Linux, use the following command line to request an SSH connection using SSH2 to the server `<remotehost>`:

```
ssh -2 <remotehost>
```

This normally returns text information that indicates the version of SSH protocol that is being used. Also, this attempts to authenticate the current user. Use the `-l username` switch to request a login as a different user.

For SiteScope running on Windows, see the section on “Testing SSH Connectivity with PuTTY Utilities” on page 1350 for information about testing SSH connectivity outside of the SiteScope application on Windows NT/2000 machines.

Once you have confirmed SSH connectivity, create or configure UNIX Remote settings in SiteScope to use SSH as the connection method.

## **Monitors Supporting Perfex/Non-Perfex Based NT SSH**

### **Monitors Supporting Perfex Based NT SSH**

The following lists the monitors that support perfex based NT SSH:

- Citrix Monitor
- ColdFusion Server Monitor
- CPU Monitor
- Directory Monitor
- Disk Space Monitor
- Memory Monitor
- Microsoft ASP Server Monitor
- Microsoft IIS Server Monitor
- Microsoft Windows Event Log Monitor
- Microsoft Windows Media Server Monitor
- Microsoft Windows Performance Counter Monitor
- Microsoft Windows Resources Monitor
- Microsoft Windows Services State Monitor
- Microsoft SQL Server Monitor
- Real Media Server Monitor
- Script Monitor
- Service Monitor

## **Monitors Supporting Non-Perfix Based NT SSH**

The following lists the monitors that support non-perfix based NT SSH:

- Citrix Monitor
- ColdFusion Server Monitor
- CPU Monitor
- Disk Space Monitor
- Memory Monitor
- Microsoft ASP Server Monitor
- Microsoft IIS Server Monitor
- Microsoft SQL Server Monitor
- Microsoft Windows Media Server Monitor
- Microsoft Windows Resources Monitor
- Real Media Server Monitor

## Troubleshooting and Limitations

This section contains troubleshooting and limitations when monitoring using SSH.

- “Skips in NT SSH Based Monitors (on Linux RedHat 5)” on page 1343
- “Non-Perfex Based NT SSH is Not Working” on page 1343
- “Non-Perfex Based SSH Fails to Retrieve Counters” on page 1344
- “Perfex Based NT SSH is Not Working” on page 1344
- “Error: "resize: unknown character exiting"” on page 1344

### **Skips in NT SSH Based Monitors (on Linux RedHat 5)**

If you encounter skips in NT SSH based monitors running on Linux RedHat 5 platforms, in the `opt/SiteScope/java/lib/security/java.security` file, you should change:

“securerandom.source=file:/ dev/urandom” to

“securerandom.source=file:///dev/urandom”

### **Non-Perfex Based NT SSH is Not Working**

If perfex based SSH is working, but non-perfex based NT SSH is not, perform the following:

- Check that perfmon is working correctly. On the target machine, run the command `perfmon` and verify that the required perfmon objects appear. For details on how to rebuild these libraries, refer to <http://support.microsoft.com/?kbid=300956>.
- Check that the remote machine has a working `typeperf` command (sample command to test) by entering the following in the command line:

```
typeperf "\Processor(_Total)\% Processor Time"
```

For details, refer to <http://technet.microsoft.com/en-us/library/cc753182.aspx>.

### **Non-Perfex Based SSH Fails to Retrieve Counters**

In some cases, non-perfex based SSH shows n/a for counters while perfmon gives the value as 0 for the same counters. This is the behavior for counters that are also not selectable using the perfmon utility. The reason that perfex is able to get values for these counters is because it bypasses perfmon and accesses them via the registry.

### **Perfex Based NT SSH is Not Working**

Check that the prerequisites for perfex based NT SSH monitoring have been met. For details, see “Install SiteScope Remote NT SSH Files” on page 1337.

### **Error: "resize: unknown character exiting"**

If SiteScope fails to create a connection using SSH and the **error.log** or **runMonitor.log** contain a server error message similar to "resize: unknown character exiting", this is probably caused by an invalid bash-related command. SiteScope supports basic bash environments only. Bash commands are usually found in the **.bashrc** file under the user default directory.



# 115

---

## Working with SSH Clients

If you need to use Secure Shell (SSH) to connect to remote UNIX or Windows servers, SiteScope must have access to a SSH client to make the connection and transmit data. This section contains some of the client configuration possibilities and issues involved in using SSH for SiteScope monitoring.

### **This chapter includes:**

#### Concepts

- Integrated Java SSH Client Overview on page 1346
- External SSH Client Overview on page 1348

#### Tasks

- Configure the Integrated Java SSH Client on page 1351
- Configure the External SSH Client on page 1355

## Integrated Java SSH Client Overview

SiteScope provides a SSH client written in Java that is integrated into the SiteScope application. This client significantly reduces the required system resources used by SiteScope when connecting to servers by using SSH. The Java client supports both SSH version 1 (SSH1) and version 2 (SSH2) protocols as well as both password-based and key-based authentication. The SiteScope configuration for the client is identical for UNIX, Linux, and Windows SiteScope.

This section includes the following topics:

- ▶ “Working with the Integrated SSH Client” on page 1346
- ▶ “Setting Up Key-Based Authentication” on page 1347
- ▶ “Using SSH Version 2 Protocol” on page 1347

### Working with the Integrated SSH Client

While SSH1 and SSH2 are both Secure Shell protocols, they are considered to be two different protocols and are not compatible with each other. Some security vulnerabilities have been found in SSH1 that has resulted in SSH2 being considered the current standard. Most SSH software supports both protocols. However, to be sure that a request for a SSH connection uses SSH2 instead of SSH1, it is necessary to configure SSH clients and SSH hosts to use the same protocol version between them to communicate. In many cases, SSH1 is the default version used for connections, as it is considered the lowest common denominator between a SSH client and a SSH host.

There are two ways to force SSH2 connections:

- ▶ **Configure all SSH daemons or servers to accept only SSH2 connection requests.** This is the most secure option but may be the most time-consuming unless each server was configured for this option when it was installed and activated.
- ▶ **Configure the SSH client on the SiteScope server to only make SSH2 requests.** Requires changes only to the client on the SiteScope server. For the integrated Java SSH client, this can be controlled by a setting in the Advanced Options section on the remote server setup page.

## Setting Up Key-Based Authentication

Another part of SSH security is authentication. The integrated SSH client for SiteScope can be configured to use one of two authentication options:

- ▶ **Password Authentication.** Password Authentication is the default method for SSH connections in SiteScope.
- ▶ **Key-Based Authentication.** Key-Based Authentication adds an additional level of security through the use of a passphrase and a public-private key authentication.

To use Key-Based Authentication for SSH remote servers, you must first create a pair of public/private keys. The public key resides on the remote and the private key is kept on the SiteScope machine. Both Cygwin OpenSSH and OpenSSH for Windows come with a key generation tool called `ssh-keygen`. The `ssh-keygen` tool allows you to create both protocol version 1 and version 2 keys. When setting up a UNIX or Windows remote server using the Internal Java Libraries Client, use the key generation tool called MindTerm to create a public/private key pair for RSA (version 1 and version 2) and DSA (version 2).

## Using SSH Version 2 Protocol

By default, the SiteScope Java client uses the SSH1 Protocol if the server it is trying to connect to allows SSH1 connections. If this negotiation fails, SiteScope attempts to connect using version 2 protocol. The SiteScope Java client can be configured to use only SSH2 connections. Making the change on the SiteScope machine may be easier than having to reconfigure a large number of remote SSH servers.

For details on configuring the Integrated Java SSH Client, see “Configure the Integrated Java SSH Client” on page 1351.

## External SSH Client Overview

SiteScope provides the capability of connecting to remote servers using an external SSH client. On Windows platforms, the plink client is included with SiteScope. On UNIX and Linux platforms, SiteScope can use a standard SSH client such as SunSSH or OpenSSH.

This section includes the following topics:

- ▶ “Working with External SSH Clients” on page 1348
- ▶ “Setting Up SSH Authentication” on page 1349
- ▶ “Monitoring with SSH on Windows Platforms” on page 1349
- ▶ “Testing SSH Connectivity with PuTTY Utilities” on page 1350
- ▶ “Setting Up SSH on SiteScope for Windows Platforms” on page 1350

### **Working with External SSH Clients**

There are two different versions of the SSH protocol: version 1 and version 2. While they are both Secure Shell protocols, they are considered to be two different protocols and are not compatible with each other. Some security vulnerabilities have been found in SSH1 that has resulted in SSH2 being considered the current standard. Most SSH software supports both protocols. However, to be sure that a request for a SSH connection uses SSH2 instead of SSH1, it is necessary to configure SSH clients and SSH hosts to use the same protocol version between them to communicate. In many cases, SSH version 1 (SSH1) is the default version used for connections, as it is considered the lowest common denominator between a SSH client and a SSH host.

There are two ways to force SSH2 connections:

- **Configure all SSH daemons or servers to accept only SSH2 connection requests.** This option is perhaps the most secure but may be the most time-consuming unless each server was configured for this option when it was installed and activated.
- **Configure the SSH client on the SiteScope server to make only SSH2 requests.** This option requires changes only to the client on the SiteScope server. For external SSH client, this is usually controlled by using the client settings.

## Setting Up SSH Authentication

Another part of SSH security is authentication. The integrated SSH client for SiteScope can be configured to use one of the following two authentication options:

- **Password Authentication.** Password Authentication is the default method for SSH connections in SiteScope.
- **Key-Based Authentication.** Key-Based Authentication adds an additional level of security through the use of a passphrase and a public-private key authentication.

## Monitoring with SSH on Windows Platforms

SiteScope for Windows platforms includes a SSH client to handle connections to remote SSH-enabled servers. SiteScope includes the PuTTY SSH utilities for SSH connectivity to both UNIX and Windows servers. These utilities are found in the <SiteScope root directory>\tools directory.

By default, SiteScope SSH connections uses the SSH1 protocol (less secure) unless the server it is connecting to accepts only SSH2 sessions. To force SiteScope to use the SSH2 protocol (more secure), you must configure the SSH client on the machine where SiteScope is running and possibly the SSH daemons/hosts on the remote servers to communicate using the SSH2 protocol. For SiteScope on Windows, configure the PuTTY SSH client utility and SiteScope as described in “Set up SSH2 on SiteScope for Windows Platforms” on page 1356.

**Note:** The PuTTY and plink tools supplied with SiteScope are not the latest release versions of these tools. SSH connectivity is handled by the internal Java libraries by default. Consider checking for newer versions and replacing the files supplied with SiteScope with updated versions. More information about the PuTTY SSH client can be found at <http://www.chiark.greenend.org.uk/~sgtatham/putty/> or <http://www.openssh.org/windows.html>.

---

## Testing SSH Connectivity with PuTTY Utilities

We recommend that you test SSH connectivity from SiteScope on Windows to remote hosts using either the **PuTTY.exe** or **plink.exe** tools. This is also useful for troubleshooting connectivity. You can use utilities to test connectivity with a SSH host. The plink utility is run from the command line.

## Setting Up SSH on SiteScope for Windows Platforms

SiteScope for the Windows platform uses plink, part of the PuTTY suite of SSH tools, to create its SSH connections for remote monitoring. By default, the plink utility uses the SSH1 Protocol if the server it is trying to connect to allows SSH1 connections. The SiteScope SSH client can be configured to use only the SSH2 protocol for connections. Making the change on the SiteScope machine may be easier than having to reconfigure a large number of remote SSH servers.

Setting up SiteScope for Windows to use only SSH2 to communicate with remote UNIX or remote Windows servers requires two actions:

- 1** Create settings in the SSH client on the SiteScope server to use only SSH2.
- 2** Modify SiteScope remote server connection profiles to use the SSH2 connection profile.

For details on configuring the external SSH2 client, see “Configure the External SSH Client” on page 1355.

## Configure the Integrated Java SSH Client

This task describes the steps involved in configuring the integrated Java SSH client.

This task includes the following steps:

- “Select an Authentication Option for SSH Connections” on page 1351
- “Configure the SiteScope Java Client to Use Only SSH2 Connections” on page 1351

### **1 Select an Authentication Option for SSH Connections**

Select an authentication option for integrating SSH client for SiteScope: password authentication (the default method in SiteScope) or key-based authentication.

For details on how to set up key-based authentication for SSH connections, see “Set Up Key-Based Authentication” on page 1352.

### **2 Configure the SiteScope Java Client to Use Only SSH2 Connections**

When configuring your remote server profile in Microsoft Windows/UNIX Remote Servers, select the **SSH version 2 only** check box in the Advanced Settings.

## **Set Up Key-Based Authentication**

This task describes the steps involved in setting up Key-Based Authentication for SSH remote servers using MindTerm.

---

**Note:** When using F-Secure, the F-Secure client creates an SEC SSH formatted key and the F-Secure server understands a SEC SSH formatted key. To use the key generated using the Internal Java Libraries client (which is in openSSH key format), you must convert the openSSH key to SEC SSH format.

---

**To create a public or private key pair:**

- 1 Open a command window on the SiteScope server, and run the following command to launch MindTerm:

```
<SiteScope root directory>\java\bin\java -jar c:\<SiteScope root directory>\WEB-INF\lib\mindterm.jar
```

---

**Note:** For SiteScope 7.9.5.x and earlier, type the command: <SiteScope root directory>\java\bin\java -jar c:\<SiteScope root directory>\java\lib\ext\mindterm.jar.

---

- 2 In MindTerm, select **File > Create Keypair > DSA (or RSA)**. Also select OpenSSH .pub format.
- 3 The key pair is written to the <USER\_HOME>\mindterm directory. Copy the **identity.pub** file to the <SiteScope root directory>\groups directory.
- 4 Copy the **identity.pub** file to the <USER\_HOME>/.ssh directory on the remote machine and rename it **authorized\_keys** (or **authorized\_keys2** for SSH2).



- 5 On the remote machine, run the following command in the `<USER_HOME>/ssh` directory, and make sure that User has read, write, and execute permissions, and that Group and Other have read permissions on the `authorized_keys` file.
- 6 Create a remote connection in SiteScope for the remote server using key file authentication and Internal Java Libraries.

The private key goes in the `<SiteScope root directory>\groups` directory and the public key in the `<USER_HOME>/ssh/authorized_keys` file on the remote machines.

The key generated from MindTerm is in **OpenSSH** format.

---

**Note:** You must verify that the server key and the MindTerm key are at the same level. For example, if the server key is 768 bit and the MindTerm key is 1024 bit, the authentication procedure fails.

---

#### To find out what your server is using:

- 1 Stop the `sshd` service on the remote server. On a Red Hat Linux server, run the command:

```
/etc/rc.d/init.d/sshd stop
```

- 2 Start the `sshd` service in debug mode on the remote server. On a Red Hat Linux server, run the command:

```
/usr/sbin/sshd -d
```

You should see output similar to **Generating 768 bit RSA key**.

---

**Note:** When using the **Key File for SSH connections** box in SiteScope, if there is a trailing space after the information entered, this causes an "unknown error (-1)" failure. Remove the trailing space to fix the problem.

---

**To convert the openSSH key to SEC SSH format:**

- 1** Create a RSA key in MindTerm (which is an openSSH key pair).
- 2** Run the following command on the remote server to convert the openSSH key to SEC SSH format:  

```
ssh-keygen -e -f <public key>
```
- 3** Leave the private key on the SiteScope server in the openSSH format.

---

**Note:** When using Key-Based authentication, the Key File supplied must be a version 2 private key.

---

## Configure the External SSH Client

This task describes the steps involved in configuring the external SSH client.

This task includes the following steps:

- “Set the SiteScope PuTTY Client to Use SSH2” on page 1355
- “Configure SiteScope to Use SSH2” on page 1356
- “Test SSH Connectivity with PuTTY Utilities” on page 1356
- “Configure SiteScope to Use SSH2” on page 1356

### 1 Set the SiteScope PuTTY Client to Use SSH2

Create settings in the SSH client on the SiteScope server to use only SSH2.

For details on how to perform this task, see “Set up SSH2 on SiteScope for Windows Platforms” on page 1356.

### 2 Select an Authentication Option for SSH Connections

Select an authentication option for integrating SSH client for SiteScope: password authentication (the default method in SiteScope) or key-based authentication.

For details on how to set up key-based authentication for SSH connections, see the instructions for creating Public Keys using the PuTTYGen tool at <http://the.earth.li/~sgtatham/putty/0.60/html/doc/Chapter8.html#pubkey>.

---

**Note:** SSH uses DES, BLOWFISH, RSA, or other public key cryptography for both connection and authentication. Public Keys are stored on a per-user basis so if you are using key-based logins instead of password-based logins, you should log in and run the PuTTYGen tool using the same account that is used by the SiteScope service.

---

### 3 Test SSH Connectivity with PuTTY Utilities

Test SSH connectivity from SiteScope on Windows to remote hosts using either the **PuTTY.exe** or **plink.exe** tools.

For details on how to perform this task, see “Test SSH Connectivity with PuTTY” on page 1358.

### 4 Configure SiteScope to Use SSH2

Modify SiteScope remote server connection profiles to use the SSH2 connection profile.

For details on how to perform this task, see “Configure SiteScope to Use SSH2” on page 1359.



### Set up SSH2 on SiteScope for Windows Platforms

This task describes the steps involved in setting up the PuTTY client on the SiteScope server to use only SSH2.

**To set up PuTTY to use SSH2:**

- 1 Log on to the server where SiteScope is running as the user who runs the SiteScope service. To see which user this is, open the Services control panel, right-click the SiteScope service, select **Properties**, and click the **Log On** tab.
- 2 Find the **PuTTY.exe** tool in the `<SiteScope root directory>\tools` directory. Alternatively, you can download an updated PuTTY version from the Internet.
- 3 Launch the PuTTY utility by double-clicking the icon in Windows Explorer (or typing **putty** in a command window with a path to the `<SiteScope root directory>\tools` directory). No installation steps are needed. The Putty Configuration console opens.
- 4 With the **Session** tab or tree selected, enter the host name or IP address of the remote machine to be monitored in the **Host Name** box. Select the SSH radio button below the host name in the Protocol section.

- 5 Select the **Connection** tab or tree, and enter the user name on the remote machine in the Auto-login user name box. This should be a user account with permissions to monitor processes and hardware statistics on the remote server. Optionally, this user account might also have execution privileges to enable SiteScope to run scripts on the remote server.
- 6 Select the **SSH** tab or tree under the Connection tree, and then choose the **2** radio button in the Preferred SSH Protocol Version section.
- 7 Return to the Session tab. In the Saved Sessions text box, enter a name for these settings. Any previously saved settings appear in the list box below.

---

**Note:** The Saved Session name should not be a resolvable host name on your network, nor can it contain a white space character. For instance, if these settings are for a machine named myhost.mydomain.com, the session settings name cannot be myhost, myhost.mydomain.com, or myhost settings (the latter is not allowed because of the white space between the words). Choose a name, such as myhost-settings.

---

- 8 Click the **Save** button. The name of your new settings should appear in the list of saved settings.
- 9 Repeat this process to create settings for each remote machine you wish to monitor with SiteScope using SSH2.

---

**Note:** Make a note of the Saved Session name for each machine that you configure, to enter this name into the SiteScope configuration file.

---

## Test SSH Connectivity with PuTTY

This task describes the steps involved in testing SSH connectivity from SiteScope on Windows to remote hosts using either the **PuTTY.exe** or **plink.exe** tools.

### To test SSH connectivity with PuTTY:

- 1 Log on to your Windows machine as the user who runs the SiteScope service.
- 2 Open a command window to the `<SiteScope root directory>\tools` directory.
- 3 Run the plink utility with the following syntax:  

```
plink -ssh <remoteuser>@<hostname>
```

where `<remoteuser>` is the login username for a valid user account on the `<hostname>` server.
- 4 Follow the prompts in the terminal window to confirm that the remote login is successful. Log out of the terminal session when you are satisfied that the connection is working correctly.

If you want to use the SSH2 protocol for connections, you must use the PuTTY utility to configure the PuTTY client to use SSH2 instead of the default SSH1. This requires that you save session settings as described in the section “Set up SSH2 on SiteScope for Windows Platforms” on page 1356. After you have done this, you can also use PuTTY to test SSH connectivity.

### To test SSH2 connectivity with PuTTY:

- 1 Log on to your Windows machine as the user who runs the SiteScope service.
- 2 Launch the PuTTY utility.
- 3 From the Session tab or tree, select the Saved Session name of the remote connection you want to test and click the **Load** button to the right of the selection box.
- 4 Click the **Open** button near the bottom of the dialog box. This launches a terminal emulation window.

- 5 Follow the prompts in the terminal window to confirm that the remote login is successful.
- 6 Log out of the terminal session when you are satisfied that the connection is working correctly.



## **Configure SiteScope to Use SSH2**

This task describes the steps involved in configuring SiteScope to use SSH2 for connecting to remote UNIX or remote Windows servers.

### **To configure SiteScope to use SSH2:**

- 1 Open SiteScope in a Web browser.
- 2 In the remote server view, right-click **Microsoft Windows/Unix Remote Servers**, and select **New Microsoft Windows/UNIX Remote Server**.
- 3 Configure the remote server settings as follows:
  - **Server.** Enter the name of the settings you saved. For example, to use the settings for myhost.mydomain.com, type myhost-settings in the box.
  - **User name.** Leave the box empty.
  - **Password.** Enter the password to log in to the remote machine.

For UNIX remote servers:

- **Operating system.** Select the applicable operating system of the target remote server.
- **Prompt.** If the shell prompt for the remote UNIX server is something other than #, enter that prompt in the box.
- **Login prompt.** Leave the box empty.
- **Password prompt.** Leave the box empty.

Click **OK** to add the remote server profile.

---

**Note:** The remote connection test fails. You may see a message similar to the following error message:

```
Connecting to myhost-settings...
Waiting for prompt(#)...
Unable to open connection:
Host does not exist
Remote command error: unknown host name (-997)
```

Go to the **<SiteScope root directory>\groups** directory and make a backup copy of the **master.config** file. Rename the backup file to **master.config.SAV**.

---

- 4 Open the **master.config** file in a text editor, and locate the section of entries or lines beginning with the string `_remoteMachine`. If you have configured multiple remote server connections, there are multiple entries that begin with this string. Locate the line that includes the string `_host=myhost-settings`, where `myhost-settings` is the name of the host settings you entered in the Server Address box in PuTTY Configuration tool.
- 5 Add the following string to the end of that line:

```
_sshCommand=<SiteScope root directory>\tools\plink.exe_-ssh_$host$_-pw_$password$
```

---

**Note:** This string must be entered on the same line. Do not add any carriage returns, new lines, or extra spaces.

---

Replace **<SiteScope root directory>** with the path to your SiteScope installation. For example, if SiteScope is installed at `C:\SiteScope`, the string would read:

```
_sshCommand=C:\SiteScope\tools\plink.exe_-ssh_$host$_-pw_$password$
```



After you have finished making modifications, the entire line should look similar to the following example:

```
_remoteMachine=_os=Linux _id=11 _trace= _method=ssh  
_password=(0x)MGJJKDKLKJNINPNJMJ _login= _host=myhost-settings  
_name= _sshCommand=C:\SiteScope\tools\plink.exe _ssh_$host$_  
pw_$password$
```

---

**Note:** This example wraps across multiple lines to fit on this page. When entering this setting into the SiteScope configuration file, be sure that it is entered all in a single line.

---

- 6** Repeat this step to modify each `_remoteMachine` entry, using the applicable host name setting created for each host using the PuTTY Configuration tool in the previous section.
- 7** Save and close the `master.config` file.
- 8** Stop and restart the SiteScope service.
- 9** Open a Web browser to the SiteScope server, and in the remote server view, click **Microsoft Windows/UNIX Remote Servers**.
- 10** In the Servers table for the remote you configured, click the **Test** button (for Windows remote servers) or **Detailed Test** button (for UNIX remote servers) to test the connection and verify that it works.



# 116

---

## UNIX Operating System Adapters

This chapter includes the main concepts, tasks, and reference information to enable SiteScope to monitor different versions of UNIX.

### **This chapter includes:**

#### Concepts

- SiteScope UNIX Operating System Adapters Overview on page 1363

#### Tasks

- Add an Adapter on page 1364

#### Reference

- UNIX Adapters Provided with SiteScope on page 1365
- Adapter File Format on page 1366
- Adapter Command List on page 1367

### **SiteScope UNIX Operating System Adapters Overview**

You can use SiteScope UNIX operating system adapters to extend SiteScope to connect to, and remotely monitor other versions of UNIX, in addition to those supported by default. This is done by configuring an adapter file to support the particular version of UNIX you want to monitor.

SiteScope uses adapter files to describe the commands that are needed to retrieve a variety of system resource information from servers running different versions of the UNIX operating system. These adapter files are written in plain text and are stored in the **SiteScope/templates.os** directory. For a list of the default UNIX adapters that are provided with SiteScope, see “UNIX Adapters Provided with SiteScope” on page 1365.

You can modify existing adapter files to adjust for specific system requirements in your environment. You can also create your own adapter files to enable SiteScope monitoring of other UNIX versions.

## Add an Adapter

This task describes the steps involved in adding an adapter to specific versions of UNIX.

### To add a UNIX adapter:

- 1 Read the Adapter Kit documentation thoroughly.
- 2 If the UNIX platform to which you want to add support is similar to one of the default SiteScope-supported UNIX platforms, make a copy of the adapter file for that UNIX version and use that as a starting point for your adapter.
- 3 Modify the adapter file to match the command line requirements for the UNIX version to which you want SiteScope to connect.
- 4 Save your adapter file to the **SiteScope/templates.os** directory. The filename must use the **.config** extension.
- 5 Open the installation SiteScope to which you have added the new adapter file.
- 6 In the left pane, click **Remote Servers** to display the remote servers view.
- 7 In the remote servers tree, right-click **UNIX Remote Servers**, and select **New UNIX Remote Server**. The New UNIX Remote Server dialog box opens.
- 8 In the **Operating system** box, select the name of the UNIX adapter that you have created.

- 9 Click **OK**. SiteScope uses the new adapter file to try and retrieve that applicable data from the remote server.
- 10 If you make changes to the adapter file after you have configured one or more server connection profiles to use the adapter, you can use the **Detailed Test** option in the UNIX Remote Servers to test your adapter. After adding the remote server, the Detailed Test displays the output of the command that SiteScope is running remotely, along with SiteScope's parsing of the output.

The amount of work required to modify a particular template depends on how different the new UNIX platform is from the supported UNIX platforms.

## UNIX Adapters Provided with SiteScope

The default UNIX adapters that are provided with SiteScope, include:

Filename	Description
<b>AIX.config</b>	Adapter file for IBM AIX
<b>Digital.config</b>	Adapter file for Digital Tru64 UNIX (Pre 4.x)
<b>FreeBSD.config</b>	Adapter file for FreeBSD 3.x
<b>HP.config</b>	Adapter file for Hewlett-Packard HP/UX
<b>HP64.config</b>	Adapter file for Hewlett-Packard HP/UX 64-bit
<b>Linux.config</b>	Adapter file for Linux (Redhat and others)
<b>MacOSX.config</b>	Adapter file for Apple MacIntosh OS X
<b>OPENSERVER.config</b>	Adapter file for SCO OpenServer
<b>SCO.config</b>	Adapter file for SCO UNIXWare
<b>SGI.config</b>	Adapter file for Silicon Graphics Irix
<b>Sun.config</b>	Adapter file for Sun Microsystems Solaris
<b>Tru64.config</b>	Adapter file for Compaq Tru64 UNIX 5.x

## Adapter File Format

Each UNIX platform supported for remote monitoring by SiteScope has an adapter file in the **SiteScope/templates.os** directory. These files use SiteScope's standard setting file format.

The first group of settings (those settings before the first # sign line) describe the platform:

```
id=yourPlatform
name=your Platform Name
```

The id is the SiteScope internal ID for the OS. This ID must be unique, contain no spaces, and can be alphanumeric. We recommend that you use the name of the adapter file as the ID name. For example, if the name of your adapter file is `linux.config`, your ID would be `linux`.

The name is the name you want displayed in the drop-down list when adding or editing remote servers.

The rest of the template file contains groups of settings representing a single command, separated by a line of # characters. For example, the following settings represent the disk space command:

```
id=disks
command=/usr/bin/df -k
mount=6
name=1
```

Where:

`id=disks` is the id that SiteScope uses to look up a command. This must be one of the set of SiteScope commands (see “Adapter Command List” on page 1367). This entry is case sensitive.

`command=/usr/bin/df -k` means that the `usr/bin/df -k` command is run to get the information about the disks.

`mount=6` and `name=1` mean that the mount name is in column 6 and the name of the mount or file system is in column 1. The data names vary from command to command and are documented below.

Applying the above for the following command output:

```
Filesystem kbytes used avail capacity Mounted on /proc 0 0 0 0%
/proc /dev/dsk/c0t3d0s0 73049 42404 23341 65% /
```

where the disks command automatically skips lines not starting with (/dev) reads column 1 (/dev/dsk/c0t3d0s0) as the name of the file system, and column 6 ("/") as the mount name.

## Adapter Command List

SiteScope requires settings for each the following commands to operate properly. Each command description requires an ID and a command, one or more fields to specify where the data is being read from, and optionally a set of modifiers that are used to filter the output of the command to eliminate certain sets of lines (such as header lines).

Where the variable column is used below, it means the number of the column in which the data appears, where columns are space delimited sets of data.

In addition, there are certain fields that can be optionally applied to any command description. For details, see “Optional Adapter Command Details” on page 1371.

### Disk Listing

ID	Description	Used by	Fields
disks	Returns a list of the file systems on the system. The /usr/bin/df -k command is the standard way to get this data. Lines returned that do not start with /dev are automatically skipped.	Disk Space Monitor	<p><b>name.</b> The column of the name of the file system.</p> <p><b>mount.</b> The column of the name of the mount.</p>

## Disk Information

ID	Description	Used by	Fields
disk	Takes a disk as an argument and returns the total, free, and percent used for the disk.	Disk Space Monitor	<p><b>total.</b> The column of the total kilobytes capacity of the file system.</p> <p><b>free.</b> The column of the free kilobytes of the file system.</p>

## Memory

ID	Description	Used by	Fields
memory	The amount of swap space used and available.	Memory Monitor	<p><b>swapUnit.</b> The multiplier applied to used, free, or total swap space to give bytes.</p> <p><b>used.</b> The amount of swap space used.</p> <p><b>free.</b> The amount of swap space free.</p> <p><b>total.</b> The amount of total swap space.</p> <p><b>Note:</b> Only two of used, free, and total fields need to read. The other is computed.</p>



## Page Faults

ID	Description	Used by	Fields
pageFault	The number of page faults/sec. If multiple page faults lines are matched, they are added up.	Memory Monitor	<p><b>pageFaults.</b> The column of the number of page faults.</p> <p><b>inPageFaults.</b> The column of the number of page in faults.</p> <p><b>outPageFaults.</b> The column of the number of page out faults.</p> <p><b>units.</b> pages (default), pages/sec, or k/sec units for the paging data.</p> <p><b>pageSize.</b> If units are k/sec, the <b>pageSize</b> is used to compute the number of pages. Otherwise it is ignored.</p> <p><b>Note:</b> Either use <b>pageFaults</b>, if there is a single column of data, or <b>inPageFaults</b> and <b>outPageFaults</b>, if there are two columns of page fault data. <b>inPageFaults</b> and <b>outPageFaults</b> are added together to get the total page faults.</p>

## CPU Usage

ID	Description	Used by	Fields
cpu	Returns the wait and idle % of the CPU.	CPU Monitor	<p><b>idle.</b> The idle % for the CPU.</p> <p><b>wait.</b> The wait % for the CPU (optional).</p>

## Process List

ID	Description	Used by	Fields
process	A list of processes with long process names. Typically this is <code>/usr/bin/ps -ef</code>	Service Monitor	<b>name.</b> The column of the names of the processes.

## Process List with Details

ID	Description	Used by	Fields
process Detail	A list of processes with size of the process. Typically this is <code>/usr/bin/ps -el</code>	Service Monitor (with Check Memory option enabled)	<b>name.</b> The column of the names of the processes <b>size.</b> The column of the size of the processes. <b>pageSize.</b> Page size on the system (optional). The default is 8192.

## Optional Adapter Command Details

The following fields can optionally be applied to any command description:

### Process List with Details

ID	Description
startLine	The line number where the command starts looking for data.
endLine	The line number where the command ends looking for data.
skipLine	The pattern that if matched, skips the line.
matchLine	The pattern that if matched, looks for data in that line.
startMatch	The pattern that if matched, starts the command looking for data.
endMatch	The pattern that if matched, ends the command looking for data.
reverseLines	If true, the command output lines are reversed and read back to front. This is useful if there is data at the end of the command and it is too difficult to work out when to start reading.

If a field name has the format, `fieldnameColumnName=COLUMN`, the adapter searches the headers (first line) for `COLUMN` and records the columns containing the data, and then use those settings to read the `fieldname` field. This is useful where the width of the columns varies, and the data has spaces in it.

For example, to read the my data information from the following command output:

```
MEM NAME DESC
12K my data some of my data
```

you would specify the name field in the command description as:

```
nameColumnName=NAME
```

The adapter reads the header line, finds `NAME`, and records where the previous column ends (`MEM` in this case) and where the specified column ends (`NAME`), and uses that to read, in this case, the text in character columns 6 through 22.

To see an example of the `ColumnName` reading in action, look at the `process` and `processDetail` commands for the supported UNIX platforms. They use this method to get the process name and the size of the process.

# Part VI

---

## Preferences



## General Preferences

This chapter includes the main concepts and reference information for SiteScope General Preferences.

**This chapter includes:**

**Concepts**

- ▶ General Preferences Overview on page 1376

**Reference**

- ▶ General Preferences User Interface on page 1379

## General Preferences Overview

This section includes the following main concepts of SiteScope General Preferences:

- “Using Default Authentication Credentials” on page 1376
- “Suspending Monitor Processes” on page 1377
- “Working with SiteScope Configuration Files” on page 1377
- “Web Script Monitor Files Directory” on page 1378
- “Setting the SiteScope Restart Schedule” on page 1378

---

**Note:** For information on general preferences relating to internationalization issues, see “Using SiteScope in an Internationalization (I18N) Environment” on page 1545.

---

### Using Default Authentication Credentials

You use this section to enter default authentication credentials that SiteScope uses to log into certain applications and systems. This user name and password are used if the following conditions are met:

- No other authentication credentials are entered as part of an individual monitor configuration.
- The target application or system requires authentication credentials. The URL Monitor, URL Sequence Monitor, and Web Service Monitor can use this function.



## Suspending Monitor Processes

In large and complex monitoring environments, it is possible that SiteScope can become heavily loaded with a large number of monitors running and the responsiveness may become slow. This may be due to some monitors being configured to monitor too aggressively or systems that are becoming overloaded. If monitoring actions are slowing the performance of SiteScope, it can be useful to temporarily suspend monitoring actions to make configuration changes. You can temporarily suspend monitors to reduce the time required to complete large configuration operations such as a global search and replace operation. The **Suspend all monitors** option provides this function.

## Working with SiteScope Configuration Files

SiteScope uses a binary monitor and system configuration data storage for the SiteScope application. This is different than versions of SiteScope earlier than 8.0.0.0 which stored monitor and system configuration data in text files in the <SiteScope root directory>\groups folder.

If you plan to manually edit the .MG files in the \groups folder, you should select the **Enable configuration files** option. If this option is not selected, SiteScope ignores changes made to these files. Disabling this option may improve SiteScope performance.

---

### Note:

- ▶ SiteScope group .MG files are still supported in SiteScope 10.10, however, the **Enable configuration files** option is no longer selected by default when SiteScope is installed. SiteScope group .MG files will be deprecated in SiteScope 11.00.
  - ▶ When upgrading from an earlier version of SiteScope that has the **Enable configuration files** option selected, the .MG configuration files are supported.
  - ▶ If you disable the **Enable configuration files** option and later want to re-enable it, you must select the option, click **Save** to save the change, and then restart SiteScope to complete the change.
-

## Web Script Monitor Files Directory

The Web Script Monitor runs VuGen scripts to monitor performance and content on Web applications. The VuGen scripts used by the monitor can be stored in the default directory for these scripts, **<SiteScope root directory>\templates.webscripts**, or you can define a different directory in General Preferences.

---

**Note:** The Web Script monitor is available only to users accessing SiteScope directly and not to users accessing SiteScope by using System Availability Management Administration in HP Business Availability Center.

---

## Setting the SiteScope Restart Schedule

Restarting the SiteScope server is necessary for clearing problems and resetting monitors. You can select a schedule used for restarting SiteScope in **Preferences > General Preferences > Main Panel**. Selecting a convenient restart schedule helps minimize or avoid gaps in monitoring coverage and data.



For details on configuring these preferences, see “General Preferences User Interface” on page 1379.

## General Preferences User Interface

<b>Description</b>	Use to enter and view licensing information, and other general display functions, optional functions, and access options for SiteScope.  <b>To access:</b> Select <b>Preferences</b> context > <b>General Preferences</b> > <b>Main Panel</b>
<b>Important Information</b>	Only an administrator in SiteScope, or a user granted <b>Edit general preferences</b> permissions, can create or make changes to General Preferences.
<b>Included in Tasks</b>	“Configure SiteScope for a Non-English Locale” on page 1547
<b>Useful Links</b>	“General Preferences Overview” on page 1376

### Main Panel

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>License number</b>	Enter SiteScope license number to register SiteScope monitors. This number is issued when purchasing a set of monitors. A license must be purchased if intending to use SiteScope beyond the trial period.
<b>License status</b>	Displays information about the license. This includes the license type, total number of monitor points permitted by the license, and how many points have been used.
<b>Monitor licenses</b>	If you have purchased licensing for optional SiteScope monitoring capabilities, click the <b>Add</b>  button and enter the license number in the Option Licenses dialog box. Generally, this license key has the same syntax as the SiteScope license. If you have purchased multiple license keys, enter each key separated with a comma. To remove a monitoring option license, select the license, and click the <b>Delete</b>  button.

GUI Element	Description
<b>VuGen scripts path root</b>	<p>Enter a directory to store the zip files of VuGen scripts for use by the Web Script Monitor. The files in the directory you enter here appear in the list of available scripts when configuring the Web Script Monitor. If you do not enter a value here, the files in the default directory <b>&lt;SiteScope root directory&gt;\templates.webscripts</b> appear when configuring the monitor.</p> <p>For details on working with the monitor, see “Web Script Monitor Overview” on page 1026.</p>
<b>Default authentication user name</b>	<p>Enter the default user name to be used for authentication with remote systems. Both <b>&lt;username&gt;</b> and <b>&lt;DOMAIN&gt;\&lt;username&gt;</b> are valid formats. SiteScope uses this user name unless a different user name is entered explicitly as part of the monitor configuration.</p>
<b>Default authentication password</b>	<p>Enter the default password to be used for authentication with remote systems. SiteScope uses this password for the monitor types listed above unless a different password is entered explicitly as part of the monitor configuration.</p>
<b>Pre-emptive authorization</b>	<p>Select an option used for authenticating the default user credentials when SiteScope requests the target URL.</p> <ul style="list-style-type: none"> <li>▶ <b>Authenticate first request.</b> Sends the username and password on the first request SiteScope makes for the target server.</li> <li>▶ <b>Authenticate if requested.</b> Sends the username and password on the second request if the server requests a username and password.</li> </ul> <p><b>Default value:</b> Authenticate first request</p>
<b>SiteScope restart schedule</b>	<p>Select the schedule used for restarting SiteScope. You can define schedules in Absolute Schedule Preferences. For details, see “Absolute Schedule Page” on page 1490.</p> <p><b>Note:</b> SiteScope must be restarted at least once every 24 hours. Any Absolute Schedule that contains an interval of more than 24 hours between schedule times is not displayed in the restart schedule list.</p> <p><b>Default value:</b> Every 24 hours after start</p>

GUI Element	Description
<p><b>Number of backups per file</b></p>	<p>Enter the number of SiteScope configuration file backups to be kept. This function helps preserve important monitor, alert, and general SiteScope configuration information. This number represents the number of backups per file that is maintained. SiteScope uses a naming convention of filename.bak.1, filename.bak.2, filename.bak.#, where 1 is the latest backup file.</p> <p><b>Example:</b> You can backup files containing general SiteScope configuration information in <code>&lt;SiteScope root directory&gt;\groups</code>.</p> <p><b>Default value:</b> 1</p>
<p><b>Locale-specific date and time</b></p>	<p>Select to have SiteScope display dates and times in a format that is applicable to a certain locale, country, or culture. To use a different locale setting, modify the SiteScope configuration file to include the codes for the desired locale and select this option in the General Preferences Settings. For details on how to perform this task, see “Configure SiteScope for a Non-English Locale” on page 1547.</p> <p><b>Default value:</b> Selected (the default is United States format)</p>
<p><b>International version</b></p>	<p>Select to enable international character sets. When this option is selected, SiteScope honors all character encoding. Use this option to instruct SiteScope to simultaneously handle character encoding from multiple sources and operating systems (for example, foreign language Web pages).</p> <p>If not selected, only the default character set of the operation system where SiteScope is installed is supported. The exceptions are all the URL monitor types, the Log File Monitor, and the File Monitor. These monitor types support multiple character encoding regardless of the International Version option setting. or details on how to perform this task, see “Configure SiteScope for a Non-English Locale” on page 1547.</p> <p><b>Default value:</b> Not selected</p>

GUI Element	Description
<p><b>Suspend all monitors</b></p>	<p>Select to temporarily suspend the execution of all monitors. Use to make configuration changes across your monitoring infrastructure. To reactivate monitoring, clear the option.</p> <p><b>Note:</b> This option disables all monitors currently defined for this SiteScope installation. If setting Suspend Monitors and later clearing this option to re-enable the monitors, the individual monitors that were set as disabled prior to the Suspend Monitors action, retain their original disabled state.</p> <p>Using this option may affect reports. Monitors that would have run during the time that monitoring was suspended may display blanks for that period in reports.</p> <p><b>Warning:</b> There is currently no visual indication in the interface that SiteScope is in a suspended monitor state. When the <b>Suspend all monitors</b> option is enabled, the following message is displayed: SiteScope is in Suspended mode; no monitors are currently running.</p> <p><b>Default value:</b> Not selected</p>
<p><b>Enable configuration files</b></p>	<p>This option enables the use of the master and monitor group configuration files for SiteScope. When enabled, SiteScope periodically checks for changes to .MG files in the <b>SiteScope\groups</b> directory and updates the binary configuration data accordingly.</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Default value:</b> Not selected</p>

## SSH Preferences

<b>Description</b>	Use to configure preferences for securely accessing a remote computer.  <b>To access:</b> Select <b>Preferences</b> context > <b>General Preferences</b> > <b>SSH Preferences</b>
--------------------	---

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>SSH V2 connect timeout (seconds)</b>	Enter the total number of seconds SiteScope should wait for a successful reply. When the time is exceeded, the connection is automatically closed.  <b>Default value:</b> 30 seconds
<b>SSH V2 hello timeout (seconds)</b>	Enter the handshake timeout (in seconds).  <b>Default value:</b> 30 seconds
<b>SSH V2 key exchange timeout (seconds)</b>	Enter the total number of seconds SiteScope should wait for SSH key exchange.  <b>Default value:</b> 30 seconds
<b>SSH V2 authentication phase timeout (seconds)</b>	Enter the total number of seconds SiteScope should wait for SSH authentication.  <b>Default value:</b> 30 seconds

## WMI Preferences

<b>Description</b>	Use to configure preferences for using Windows Management Instrumentation (WMI) to access a remote computer. WMI is a more secure communication method than NetBIOS for gathering data from remote servers running on Windows servers.  <b>To access:</b> Select <b>Preferences</b> context > <b>General Preferences</b> > <b>WMI Preferences</b>
<b>Included in Tasks</b>	“Configure the WMI Service for Remote Monitoring” on page 1284
<b>Important Information</b>	“Monitors Supporting Windows Management Instrumentation (WMI)” on page 343

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>SiteScope NT Localhost method</b>	Select the connection type method (NetBIOS or WMI) for monitoring Windows server resources on the localhost machine.  <b>Default value:</b> NetBIOS
<b>WMI query timeout (seconds)</b>	Enter the WMI query timeout, in seconds, for each monitor run. If this box is empty, the timeout is 120 seconds.  <b>Default value:</b> 120 seconds



## Dashboard Monitor History View Options

<b>Description</b>	<p>You configure Monitor History to view monitor history on all monitors and monitor groups.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>General Preferences</b> &gt; <b>Dashboard Monitor History View Options</b></p>
<b>Important Information</b>	<p>In the Dashboard layout, you can then use a filter to further limit the monitors displayed to those that meet selected criteria. Your preferences are saved with the Dashboard filter settings. For details, see “Dashboard Filter Overview” on page 1849.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Enable monitor history view</b>	<p>Select to enable Monitor History in Dashboard. Disabling this option after it has been enabled deletes all the view data displayed in the history view.</p> <p><b>Default value:</b> Not selected</p>
<b>Display data collected during time period</b>	<p>Select the time frame for displaying past runs. Older runs are dropped. This setting overrides any dashboard filtering.</p> <p><b>Default value:</b> Past 1 hour</p>
<b>Monitor run status</b>	<p>Select the required run status. Runs with other statuses are dropped. This setting overrides any dashboard filtering.</p> <p><b>Default value:</b> Any</p>
<b>Maximum number of runs to display</b>	<p>Enter the number of rows of data to keep in memory.</p> <p><b>Default value:</b> 100000</p> <p><b>Minimum value:</b> 1000</p>

## JDBC Global Options

<b>Description</b>	<p>Use to apply global JDBC options to the following resources that connect to the database:</p> <ul style="list-style-type: none"> <li>➤ SiteScope database logger</li> <li>➤ Database tools (Database Connection, Database Information)</li> <li>➤ Database alerts</li> <li>➤ Database monitors (Oracle Database, Database Counter, Database Query, DB2 8.x and 9.x, Technology Database Integration)</li> </ul> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>General Preferences</b> &gt; <b>JDBC Global Options</b></p>
--------------------	---

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Connection timeout</b>	<p>The amount of time, in seconds/minutes/hours/days, to wait for a new SQL connection to be made. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored.</p> <p><b>Default value:</b> 5 minute</p>
<b>Driver trace log file</b>	<p>Used to create a driver trace log file for troubleshooting database drivers. This box is empty by default, and we recommend that you use it only for troubleshooting.</p> <p>To create the log file, enter the full path or UNC name of the driver trace file (for example, e:\mydir\myfile.log).</p> <p><b>Note:</b> The target log file can contain login information, table names and queries.</p>

---

## Infrastructure Preferences

This chapter includes the main concepts and reference information for SiteScope Infrastructure Preferences.

### **This chapter includes:**

#### Concepts

- ▶ Infrastructure Preferences Overview on page 1387

#### Reference

- ▶ Infrastructure Preferences User Interface on page 1388

### **Infrastructure Preferences Overview**

Infrastructure Preferences enable you to view and define global SiteScope settings without having to access the **master.config** file. Infrastructure Preferences are sorted and grouped into the following categories: General Settings, Server Settings, Monitor Settings, Alert Settings, Template Settings, Persistency Settings, Report Settings, Baseline Settings, Dashboard Settings, and Custom Settings.

After you edit setting values in Infrastructure Preferences, SiteScope validates that all input data is in the correct format and warns you if restarting SiteScope is required. You can restart SiteScope from the Infrastructure Settings page.

For details on configuring infrastructure preference values, see “Infrastructure Preferences User Interface” on page 1388.

## Infrastructure Preferences User Interface

<b>Description</b>	Enables you to define the values of settings that determine how SiteScope runs.  <b>To access:</b> Select <b>Preferences</b> context > <b>Infrastructure Preferences</b>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit infrastructure preferences</b> permissions can create or make changes to SiteScope Preferences and restart SiteScope from Infrastructure Preferences.</li> <li>▶ Most Custom settings do not have a user-friendly text label and are listed only by their corresponding property name from the <b>master.config</b> file.</li> </ul>
<b>Useful Links</b>	“Infrastructure Preferences Overview” on page 1387

### General Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Accept untrusted SSL certificates</b>	Allows SiteScope to accept any untrusted certificate when SSL is used. Otherwise, only certificates specified in the keystore file or that have a trust chain leading to a registered CA certificate are accepted.  <b>Default value:</b> Not selected <b>Property name:</b> <code>_sslAcceptAllUntrustedCerts</code>
<b>Allow Unix to NT</b>	Allows using remote Windows servers if SiteScope is running on UNIX.  <b>Default value:</b> Not selected <b>Note:</b> <ul style="list-style-type: none"> <li>▶ Only the Microsoft Windows Performance Counter monitor is supported.</li> <li>▶ You must restart SiteScope if you change this setting.</li> </ul> <b>Property name:</b> <code>_allowUnixToNT</code>

GUI Element	Description
<b>Disable quotes for cmd.exe</b>	<p>Avoids wrapping parameters in quotes when running cmd.exe for various tasks.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> _disableDoubleQuotesInTemplates</p>
<b>DNS name tags</b>	<p>A comma-separated list of values considered by DNS-related functionality as the DNS "name" tag.</p> <p><b>Default value:</b> Name;,Nombre;,Navn;,Nome;,Nom ;,Nom\u00FF:</p> <p><b>Property name:</b> _dnsNameTags</p>
<b>DNS server tags</b>	<p>A comma-separated list of values considered by DNS-related functionality as the DNS "server" tag.</p> <p><b>Default value:</b> Server;,Servidor;,Serveur;,Serveur\u00FF:</p> <p><b>Property name:</b> _dnsServerTags</p>
<b>Don't check default thresholds</b>	<p>SiteScope checks monitor results against user selected thresholds only and not against the default SiteScope monitor thresholds.</p> <p><b>Default value:</b> Selected</p> <p><b>Property name:</b> _noCheckDefaultThresholds</p>
<b>Email character set</b>	<p>These properties set the character set for email generated by SiteScope in Email Preferences and Email alerts.</p> <p><b>Default value:</b> If no value is entered, UTF-8 is used.</p> <p><b>Property name:</b> _mailCharSet</p>
<b>Email subject character set</b>	<p>These properties set the subject character set for email generated by SiteScope in Email Preferences and Email alerts.</p> <p><b>Default value:</b> If no value is entered, UTF-8 is used.</p> <p><b>Property name:</b> _mailSubjectCharSet</p>
<b>Enable report credentials to BAC</b>	<p>If selected, SiteScope sends the credentials of any host to HP Business Availability Center.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> _sendCredentials</p>

GUI Element	Description
<b>Log only enabled monitors</b>	<p>SiteScope does not log runs for disabled monitors in the daily log files.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> <code>_onlyLogEnabledMonitors</code></p>
<b>Maximum idle threads per pool</b>	<p>The maximum number of idle threads allowed per thread pool.</p> <p><b>Default value:</b> 100</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_threadPoolMaxIdle</code></p>
<b>Maximum processes per pool</b>	<p>The maximum number of processes allowed per process pool.</p> <p><b>Default value:</b> 200</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_processPoolMaxPerPool</code></p>
<b>Monitor delay between refresh (milliseconds)</b>	<p>The amount of time, in milliseconds, to wait before running a monitor after it has already been run since startup.</p> <p><b>Default value:</b> 1000 milliseconds</p> <p><b>Property name:</b> <code>_monitorDelayBetweenRefresh</code></p>
<b>NT SSH timeout (seconds)</b>	<p>The number of seconds to wait for an SSH connection to remote Windows servers before timing out.</p> <p><b>Default value:</b> 0 seconds</p> <p><b>Property name:</b> <code>_NTSSHTimeout</code></p>
<b>Number of open port tries</b>	<p>The maximum number of attempts to open a reserved port in the 811-1024 range for rlogin and rsh remote access methods.</p> <p><b>Default value:</b> 25</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_localPortRetryCount</code></p>

GUI Element	Description
<b>Numeric values format</b>	<p>The format of numeric values when converting to string representation.</p> <p><b>Default value:</b> #.##</p> <p><b>Property name:</b> _noScientificNotation</p> <p><b>Tip:</b> For more detailed information on numeric values format, refer to the HP Software Self-solve knowledge base (<a href="http://h20230.www2.hp.com/selfsolve/document/KM305059">http://h20230.www2.hp.com/selfsolve/document/KM305059</a>). To enter the knowledge base, you must log in with your HP Passport ID.</p>
<b>Perfex process maximum idle time (milliseconds)</b>	<p>The amount of time, in milliseconds, to wait before SiteScope cleans idle perfex processes. Cleaning processes improves the memory footprint on the SiteScope machine.</p> <p><b>Default value:</b> 10 minutes</p> <p><b>Property name:</b> _perfexProcessMaxIdleTime</p>
<b>Perfex timeout (seconds)</b>	<p>The number of seconds for perfex to attempt to make a connection or to attempt to run a monitor before timing out.</p> <p><b>Default value:</b> 120 seconds</p> <p><b>Property name:</b> _perfexTimeout</p>
<b>Process pool kill timeout (milliseconds)</b>	<p>The number of milliseconds to wait before SiteScope kills a non-responsive process. This is to avoid killing processes on every timeout.</p> <p><b>Default value:</b> 60000 milliseconds (the maximum recommended value is 180000 milliseconds)</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> _processPoolKillTimeout</p>

GUI Element	Description
<b>Recursive 'depends on'</b>	<p>Allows recursion in the monitor <b>Depends on</b> box. This means that subgroups become disabled when the parent group is disabled because of a dependency. By default, only the immediate group impacted by the dependency is disabled.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_dependsOnRecursive</code></p>
<b>Send remote server display name to BAC</b>	<p>Sends the remote server display name to HP Business Availability Center instead of the remote server host name. It is preferable to use this setting when DNS resolution is disabled.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> <code>_sendRemoteServerDisplayNameToBAC</code></p>
<b>SiteScope sleep delay (milliseconds)</b>	<p>The amount of time, in milliseconds, of the sleep interval in the main thread.</p> <p><b>Default value:</b> 180 milliseconds</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_monitorProcessCheckDelay</code></p>
<b>SiteScope tree refresh rate (in seconds)</b>	<p>The amount of time, in seconds, to wait between refreshing the SiteScope tree. The minimum value is 30 seconds.</p> <p><b>Default value:</b> 60 seconds</p> <p><b>Property name:</b> <code>_sisTreeRefreshRateSecs</code></p>
<b>Sleep interval on error (milliseconds)</b>	<p>The amount of time, in milliseconds, to wait before rerunning a monitor using the <b>Verify error</b> option.</p> <p><b>Default value:</b> 5000 milliseconds</p> <p><b>Property name:</b> <code>_verifySleepDuration</code></p>



GUI Element	Description
<b>Thread pool maximum idle time (milliseconds)</b>	<p>The amount of time, in milliseconds, to wait before SiteScope cleans idle thread pools.</p> <p><b>Default value:</b> 600000 milliseconds (10 minutes)</p> <p><b>Property name:</b> <code>_threadPoolMaxIdleTime</code></p>
<b>Time zone offset</b>	<p>Manually sets the time zone offset, in hours, from Greenwich Mean Time (GMT). You can enter both positive and negative, integer and non-integer values.</p> <p><b>Default value:</b> -999 (no offset)</p> <p><b>Example:</b> In Eastern US (EST), the time zone offset is GMT -5.</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_timeZoneOffset</code></p>
<b>Topology resolving frequency (minutes)</b>	<p>The amount of time, in minutes, to wait between checking the topology of the server being monitored. If this time is exceeded during a monitor run, the monitor creates the topology again in Business Availability Center's CMDB.</p> <p><b>Default value:</b> 120 minutes</p> <p><b>Property name:</b> <code>_topologyResolvingFrequencyInMinutes</code></p>
<b>Traceroute command</b>	<p>(For Unix) Specify the path to the traceroute command to override the default for the platform.</p> <p><b>Default value:</b> No value</p> <p><b>Property name:</b> <code>_tracerouteCommand</code></p>

## Server Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Host name override</b>	Allows overriding of the SiteScope host name for Business Availability Center. <b>Default value:</b> No value <b>Property name:</b> <code>_sisHostNameOverride</code>
<b>Kill processes</b>	Allows SiteScope to kill its child processes when the SiteScope process is stopped. <b>Default value:</b> Selected <b>Property name:</b> <code>_killProcesses</code>
<b>Maximum monitor processes</b>	The maximum number of monitor processes in the process pool. <b>Default value:</b> 100 <b>Note:</b> You must restart SiteScope if you change this setting. <b>Property name:</b> <code>_maxMonitorProcesses</code>
<b>Maximum monitor running</b>	The maximum number of running monitor processes in the queue. <b>Default value:</b> 400 <b>Note:</b> You must restart SiteScope if you change this setting. <b>Property name:</b> <code>_maxMonitorsRunning</code>
<b>Maximum monitor skips</b>	The maximum number of consecutive monitor skips allowed before a monitor is disabled or SiteScope is shut down. <b>Default value:</b> 10 <b>Note:</b> You must restart SiteScope if you change this setting. <b>Property name:</b> <code>_maxMonitorSkips</code>

GUI Element	Description
<b>Shutdown on monitor skips</b>	<p>SiteScope shuts down with an error if a monitor exceeds its maximum allowed skip count.</p> <p><b>Default value:</b> Selected</p> <p><b>Property name:</b> _shutdownOnSkips</p>
<b>SiteScope restart timeout for UNIX machines (minutes)</b>	<p>The maximum time allowed for SiteScope to restart itself on UNIX machines.</p> <p><b>Default value:</b> 15 minutes</p> <p><b>Property name:</b> _restartTimeout</p>
<b>SiteScope shutdown timeout (seconds)</b>	<p>The amount of time, in seconds, that SiteScope should wait to shutdown before timing out.</p> <p><b>Default value:</b> 60 seconds</p> <p><b>Property name:</b> _shutdownTimeout</p>
<b>Startup script</b>	<p>Runs this script whenever SiteScope starts up, regardless of the platform or procedure used to start SiteScope. (Empty=none)</p> <p><b>Default value:</b> No value</p> <p><b>Property name:</b> _startupScript</p>

## Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Additional error tokens</b>	<p>Additional list of keywords that should be handled as signs of failure during server output parsing.</p> <p><b>Default value:</b> Failed to .* Error code:</p> <p><b>Property name:</b> _scriptMonitorErrorMsgs2</p>
<b>Browsable EXE timeout (milliseconds)</b>	<p>The maximum amount of time, in milliseconds, to wait for retrieving counter information and for running the monitor. This setting only applies to executable-based browsable monitors, such as SAP, Sybase, and DB2 8.x and 9.x monitors.</p> <p><b>Default value:</b> 45000</p> <p><b>Property name:</b> _browsableExeTimeout</p>
<b>Browsable monitors - In error, send status of all counters to BAC</b>	<p>When a browsable monitor is in error status, SiteScope only sends the list of counters in error and their current values to BAC. At other times (when the monitor is in good status), SiteScope forwards all the counter names and values to BAC.</p> <p>If selected, SiteScope sends all the counters (the ones in error, and the ones with good status) and their values to BAC even during error.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> _isSendStatusOfAllBrowsableCountersToBAC</p>
<b>CPU error at 100%</b>	<p>The CPU monitor switches to the default error status when CPU utilization reaches 100% on the target machine.</p> <p><b>Default value:</b> Selected</p> <p><b>Property name:</b> _cpuEnableErrorAt100</p>

GUI Element	Description
<b>CPU maximum units</b>	<p>The maximum number of CPU units supported by the CPU monitor.</p> <p><b>Default value:</b> 16</p> <p><b>Property name:</b> <code>_cpuMaxProcessors</code></p>
<b>DB maximum columns</b>	<p>The maximum number of columns processed by DB monitors.</p> <p><b>Default value:</b> 10</p> <p><b>Property name:</b> <code>_databaseMaxColumns</code></p>
<b>DB maximum rows</b>	<p>The maximum number of rows processed by DB monitors.</p> <p><b>Default value:</b> 1</p> <p><b>Property name:</b> <code>_databaseMaxRows</code></p>
<b>DB maximum value length</b>	<p>The maximum length, in characters, of the data processed by DB monitors.</p> <p><b>Default value:</b> 200</p> <p><b>Property name:</b> <code>_databaseMaxSummary</code></p>
<b>Default precision</b>	<p>The default precision for floating-point values processed by some monitors.</p> <p><b>Default value:</b> 0 (disabled)</p> <p><b>Property name:</b> <code>_defaultPrecision</code></p>
<b>Dialup options</b>	<p>Options for <code>dialup.exe</code> when running it from the Microsoft Windows Dial-up monitor. Set to <code>-silent</code> to have the modem dial silently. Set to <code>-debug</code> to enable dialup debugging.</p> <p><b>Default value:</b> 0</p> <p><b>Property name:</b> <code>_dialupOptions</code></p>
<b>Empty last line reading</b>	<p>Includes the last empty line in the Script monitor output.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> <code>_enable_script_monitor_non_empty_last_line_reading</code></p>

GUI Element	Description
<b>Enable JDBC logging</b>	<p>Enables JDBC search results logging for the Link Check monitor.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> <code>_linkMonitorJdbcEnabled</code></p>
<b>Enable/Disable description mandatory</b>	<p>Enables you to make adding a description a required field when enabling or disabling an alert or monitor.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> <code>_enableDisableDescriptionMandatory</code></p>
<b>Error tokens for Script monitor</b>	<p>List of keywords that should be handled as signs of failure during server output parsing.</p> <p><b>Default value:</b> not found, Not Found, denied, Denied, cannot execute such file or directory</p> <p><b>Property name:</b> <code>_scriptMonitorErrorMsgs</code></p>
<b>Event log messages to save</b>	<p>The number of Microsoft Windows Event Log descriptions to save when saving diagnostic text for alerts.</p> <p><b>Default value:</b> 10</p> <p><b>Property name:</b> <code>_eventLogMessagesToSave</code></p>
<b>Exclusive monitor timeout (seconds)</b>	<p>The maximum amount of time, in seconds, that exclusive monitors must wait for other monitors to finish before running. The only monitor affected by this is the Microsoft Windows Dial-up monitor.</p> <p><b>Default value:</b> 120 seconds</p> <p><b>Property name:</b> <code>_exclusiveMonitorTimeout</code></p>
<b>FTP content match maximum size</b>	<p>The maximum size of the buffer used to match FTP content.</p> <p><b>Default value:</b> 50000</p> <p><b>Property name:</b> <code>_ftpContentMatchMax</code></p>

GUI Element	Description
<b>FTP download limit</b>	<p>The maximum number of bytes downloaded from each file to match.</p> <p><b>Default value:</b> -1 (no limit)</p> <p><b>Property name:</b> <code>_ftpDownloadLimit</code></p>
<b>FTP maximum threads</b>	<p>The maximum number of simultaneous FTP worker threads allowed.</p> <p><b>Default value:</b> 1</p> <p><b>Property name:</b> <code>_ftpMaxThreads</code></p>
<b>HTTP content match display limit</b>	<p>The maximum number of bytes to display for URL monitor content match.</p> <p><b>Default value:</b> 150</p> <p><b>Property name:</b> <code>_urlContentMatchDisplayMax</code></p>
<b>HTTP content match limit</b>	<p>The maximum number of bytes to check for URL monitor content match.</p> <p><b>Default value:</b> 50000</p> <p><b>Property name:</b> <code>_urlContentMatchMax</code></p>
<b>Initial monitor delay (seconds)</b>	<p>The time, in seconds, over which to randomly schedule monitor updates after a SiteScope restart.</p> <p>When changing a monitor's frequency so that its next run occurs immediately (for example, if a monitor has not run in 5 minutes, and you change the frequency to less than 5 minutes), SiteScope randomly schedules the next run during the specified period.</p> <p><b>Default value:</b> 600 seconds</p> <p><b>Property name:</b> <code>_initialMonitorDelay</code></p>
<b>Keep Astra log files</b>	<p>Allows the Astra monitor to keep Astra log files.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> <code>_astraKeepLogFiles</code></p>

GUI Element	Description
<b>Mail attachment content support base64</b>	<p>Supports mail attachment content-transfer-encoding with base64 for the Mail monitor.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> _mailAttachmentBase64Support</p>
<b>Maximum BMC counters</b>	<p>The maximum number of BMC Patrol counters the monitor is allowed to retrieve.</p> <p><b>Default value:</b> 50</p> <p><b>Property name:</b> _browsableBMCCContentMaxCounters</p>
<b>Maximum browsable counters to be selected</b>	<p>The maximum number of browsable counters that can be selected from the browsable tree.</p> <p><b>Default value:</b> 100</p> <p><b>Property name:</b> _browsableContentMaxCounters</p>
<b>Maximum Windows Performance Counter monitor counters</b>	<p>The maximum number of counters allowed for each instance of a Microsoft Windows Performance Counter monitor.</p> <p><b>Default value:</b> 8</p> <p><b>Property name:</b> _NTCounterMonitorMaxCounters</p>
<b>Microsoft Windows Media Server monitor service names</b>	<p>Enter the service names to monitor using the Microsoft Windows Media Server monitor.</p> <p><b>Default value:</b> Windows Media Services (this includes Windows Media Station Service and Windows Media Unicast) Service)</p> <p><b>Property name:</b> _counterObjectsWindowsMediaMonitor</p>
<b>MS Media Player 9 account blocked</b>	<p>Select this option and add the account directory path to the <b>MS Media Player 9 account directory</b> box if your Media Player account stops working with a 17999 error.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> _MediaPlayer9AccountBlocked</p>



GUI Element	Description
<b>MS Media Player 9 account directory</b>	<p>Enter the Media Player account directory if you get a 17999 error for the Media Player monitor.</p> <p><b>Example:</b> C:\Documents and Settings\&lt;&lt;USER&gt;\Local Settings\Application Data\Microsoft\Windows Media\9.0</p> <p><b>Property name:</b> _MediaPlayer9AccountBlockedDir</p>
<b>Network Bandwidth monitor sanity check</b>	<p>Performs a sanity check on the Network Bandwidth monitor.</p> <p><b>Default value:</b> Selected</p> <p><b>Property name:</b> _performNetworkBandwidthSanityCheck</p>
<b>Real Media Server monitor service names</b>	<p>Enter the service names to monitor using the Real Media Server monitor.</p> <p><b>Default value:</b> RMServer</p> <p><b>Property name:</b> _counterObjectsRealMonitor</p>
<b>Run script through perfex tool</b>	<p>Runs the script through the perfex tool.</p> <p><b>Default value:</b> Selected</p> <p><b>Property name:</b> _scriptRunThroughPerfex</p>
<b>Script monitor output limit</b>	<p>The number of lines to save from Script output after launching the Script monitor.</p> <p><b>Default value:</b> 25</p> <p><b>Property name:</b> _scriptMonitorLinesToSave</p>
<b>Script monitor replacement strings</b>	<p>Stores a list of space-separated strings which are parameter tags in the remote script. When the Script monitor is run, it replaces parameters tags from the script command with actual parameter values from monitor preferences.</p> <p><b>Default value:</b> \$ %</p> <p><b>Property name:</b> _scriptMonitorReplacementChars</p> <p><b>Example:</b> If the script command is test \$ %, replacement chars are \$ %, and parameters are Param1 Param2, the monitor runs the following command: test Param1 Param2.</p>

GUI Element	Description
<b>Simultaneously running DNS monitors</b>	<p>The maximum number of DNS monitors that can run simultaneously. This is relevant only when using the <b>roundTripTime</b> counter. The NSLookup operation can load the operating system and affect the values.</p> <p><b>Default value:</b> 0 (0 means that the number of simultaneous DNS monitors is unlimited)</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_maxDnsMonitorsRunning</code></p>
<b>SNMP monitors maximum number</b>	<p>The maximum number of SNMP monitors that can run at any given time.</p> <p><b>Default value:</b> 10</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_snmpMonitorMaximum</code></p>
<b>SNMP Trap encoding</b>	<p>SNMP Trap encoding for the SNMP Trap monitor. Empty=ISO8859-1.</p> <p><b>Default value:</b> ISO8859-1</p> <p><b>Property name:</b> <code>_snmpTrapEncoding</code></p>
<b>SNMP Trap monitor log limit</b>	<p>The maximum number of lines to look through SNMP Trap log for the SNMP Trap monitor. This box is filled only if <b>Run Alerts</b> is set to <b>Once, after all SNMP Traps have been checked</b> in the SNMP Trap monitor page.</p> <p><b>Note:</b> Setting a high limit may increase the size of the <b>SiteScope.log</b> or <b>RunMonitor.log</b>.</p> <p><b>Default value:</b> 1000</p> <p><b>Property name:</b> <code>_SNMPTrapMonitorDetailsMax</code></p>

GUI Element	Description
Use DNS Java library	Use the DNS Java library. <b>Default value:</b> Not selected <b>Property name:</b> _useDNSJava
Web Service monitor: maximum read length (bytes)	The maximum amount of data, in bytes, to read from the log file for the Web Server monitor. <b>Default value:</b> 50000 bytes <b>Property name:</b> _maxAmountToRead

### Alert Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Alert attempt delay (seconds)	The number of seconds to wait between each attempt to send a Post Alert. <b>Default value:</b> 120 seconds <b>Property name:</b> _postAttemptDelay
Maximum alert threads	The maximum number of alert threads in the pool. <b>Default value:</b> 100 <b>Property name:</b> _threadPoolAlertMaxThreads
Maximum runs for Post action	The maximum number of attempts to send a Post Alert. <b>Default value:</b> 4 <b>Property name:</b> _postAttempts
Maximum script alert processes	The maximum number of Script Alert processes that are allowed to run simultaneously. <b>Default value:</b> 25 <b>Property name:</b> _maxScriptAlertProcesses

GUI Element	Description
<b>Maximum sound alert length (milliseconds)</b>	The maximum length of time, in milliseconds, of the Sound Alert sound. <b>Default value:</b> 0 <b>Property name:</b> _AudioSleepTime
<b>Pager delay (seconds)</b>	The delay between pager signals when using a Pager Alert. <b>Default value:</b> 5 <b>Property name:</b> _delayBetweenPages

## Template Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Allow creation of template monitors directly under template entity</b>	<p>Enables you to add a monitor directly under a template without creating a group in the template.</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Default value:</b> Not selected</p> <p><b>Property name:</b> _allowTemplateMonitorDirectlyUnderTemplate</p>

## Persistency Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Maximum changes per persistency delta file</b>	<p>The maximum number of persistency changes kept in each persistency delta file.</p> <p><b>Default value:</b> 51</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> _PersistencyMaxChangesInDeltaFile</p>
<b>Maximum persistence history items</b>	<p>The maximum number of history items kept in persistence.</p> <p><b>Default value:</b> 1000</p> <p><b>Property name:</b> _PersistencyMaxHistoryItems</p>

GUI Element	Description
<p><b>Maximum persistence history size</b></p>	<p>The maximum size of persistence history in bytes.  <b>Default value:</b> 20000  <b>Note:</b> You must restart SiteScope if you change this setting.  <b>Property name:</b> _PersistencyMaxHistorySize</p>
<p><b>Maximum temp directory size</b></p>	<p>The maximum size, in kilobytes, of the temp directory.  <b>Default value:</b> 10000  <b>Note:</b> You must restart SiteScope if you change this setting.  <b>Property name:</b> _tempDirMaxSize</p>

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Default time length for report (hours)</b>	The default time period for including monitoring data in a Quick or Alert report. <b>Default value:</b> 1 hour <b>Property name:</b> <code>_quickReportDefaultTimePeriod</code>
<b>Include alert.log.old in report</b>	Includes the <b>alert.log.old</b> file in the Alert Report. <b>Default value:</b> Selected <b>Property name:</b> <code>_includeAlertLogOld</code>
<b>Maximum errors in monitor history report</b>	The maximum number of errors shown in the monitor history report. <b>Default value:</b> 100 <b>Property name:</b> <code>_maxReportErrors</code>
<b>Maximum samples in the history report</b>	The maximum number of samples (readings or lines) in the history report. <b>Default value:</b> 100 <b>Property name:</b> <code>_reportMaxBuckets</code>
<b>Maximum warnings in monitor history report</b>	The maximum number of warnings shown in the monitor history report. <b>Default value:</b> 100 <b>Property name:</b> <code>_maxReportWarnings</code>
<b>Use advanced sampling algorithm in report</b>	Defines the time between samples in the report as the minimum of all reported monitor frequencies. <b>Default value:</b> Not selected <b>Property name:</b> <code>_useReportAdvancedSamplingAlgorithm</code>

## Baseline Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Activation thread priority</b>	<p>The priority assigned to the activation thread. The priority, if specified, must be between 1-10, inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baselines are activated. Keep the priority as low as possible, so as not to interfere with SiteScope online functionality.</p> <p><b>Default value:</b> 1 (low priority)</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_baseliningActivationThreadPriority</code></p>
<b>Automatically create an error boundary if no error thresholds are defined</b>	<p>Automatically creates a baseline threshold using the error boundary offset value when no error thresholds have been defined for a monitor.</p> <p><b>Default value:</b> Selected</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_baseliningAutomateUpperBoundCreation</code></p>
<b>Calculation thread priority</b>	<p>The priority assigned to the calculation thread. The priority, if specified, must be between 1-10 inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baseline calculations take to complete. Keep the priority as low as possible, so as not to interfere with SiteScope online functionality.</p> <p><b>Default value:</b> 1 (low priority)</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_baseliningCalculationThreadPriority</code></p>



GUI Element	Description
<b>Failed parsings handler thread priority</b>	<p>The priority assigned to the failed parsing thread handler. The priority, if specified, must be between 1-10 inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baseline calculations take to complete. Keep the priority as low as possible, so as not to interfere with SiteScope online functionality.</p> <p><b>Default value:</b> 1 (low priority)</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> _baseliningFailedParsingHandlerThreadPriority</p>
<b>Include today's data in calculation</b>	<p>Specifies whether to include the current day's data in the baseline calculation.</p> <p><b>Default value:</b> Selected</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> _baseliningCalculationIncludesToday</p>
<b>Interval for saving accumulated baseline data to disk (minutes)</b>	<p>The interval, in minutes, used by SiteScope to save baseline data accumulated in the memory to the disk. A shorter interval reduces the memory consumption, but increases the vulnerability to failures and reduces performance.</p> <p><b>Default value:</b> 30 minutes</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> _baseliningSaveAccumulatedDataIntervalMinutes</p>

GUI Element	Description
<p><b>Maximum number of days to include in calculation</b></p>	<p>The number of days of historical data that are included in baseline calculations. The higher the number, the more precise the baseline result, but the calculation takes more time and uses more disk space. Data that is older than this value is not included in the calculation. For more details on the calculation model, see “How SiteScope Calculates Thresholds” on page 320.</p> <p><b>Default value:</b> 30 days</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_baseliningDaysToIncludeInCalculation</code></p>
<p><b>Maximum number of percentile ranges</b></p>	<p>Limits the number of percentile ranges displayed in the Percentile Ranges Mapping Table.</p> <p><b>Default value:</b> 8</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_baseliningMaxNumberOfPercentilesRanges</code></p>
<p><b>Minimum number of days required for baselining</b></p>	<p>The minimum number of days that the monitors must have run for SiteScope to calculate the baseline.</p> <p><b>Default value:</b> 14 days</p> <p><b>Minimum value:</b> 1 (if you enter a value of less than 1, the default value is used instead).</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_baseliningMinimumNumberOfDays</code></p>

GUI Element	Description
<b>Minimum number of samples required for baselining</b>	<p>The minimum number of samples required for SiteScope to calculate the baseline.</p> <p><b>Default value:</b> 2016 (the number of samples produced for a monitor running over a two week period, where the monitor runs every 10 minutes)</p> <p><b>Minimum value:</b> 1 (if you enter a value of less than 1, the default value is used instead).</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_baseliningMinimumNumberOfSamples</code></p>
<b>Offset for calculating error boundary</b>	<p>Specifies the offset value to use for calculating the error boundary. The baseline threshold is multiplied by this value when:</p> <ul style="list-style-type: none"> <li>▶ The <b>Automatically create Error Threshold Boundary if no error thresholds are defined</b> option is selected (see below), or</li> <li>▶ The current most extreme error threshold is less extreme than the calculated baseline threshold.</li> </ul> <p><b>Default value:</b> 0.3</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_baseliningUpperBoundOffset</code></p>
<b>Parsing chunk size</b>	<p>Specifies the number of monitors that are handled simultaneously by the log file parser. The higher the number, the faster the baselining calculation, but more file handlers are used.</p> <p><b>Default value:</b> 100</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> <code>_baseliningParsingChunkSize</code></p>

GUI Element	Description
<p><b>Parsing thread priority</b></p>	<p>The priority assigned to the parsing thread. The priority, if specified, must be between 1-10 inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baseline calculations take to complete. Keep the priority as low as possible, so as not to interfere with SiteScope online functionality.</p> <p><b>Default value:</b> 1 (low priority)</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> _baseliningParsingThreadPriority</p>
<p><b>Percentile of discarded samples</b></p>	<p>The percentile of the most extreme samples (considered "noise" measurement samples) that are not included in the baseline calculation.</p> <p><b>Default value:</b> 2.0</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Property name:</b> _baseliningNoiseMarginPercentile</p>

## Custom Settings

---

**Note:** Most Custom settings do not have a user-friendly text label and are listed only by their corresponding property name from the **master.config** file. These settings are not included in the documentation.

---

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Auto Deployment Check Frequency (seconds)</b>	<p>The time interval in seconds that the auto template deployment xml files in the <b>persistence\autodeployment</b> directory are deployed. For details on the feature, see “Auto Template Deployment” on page 1643.</p> <p><b>Default value:</b> 120</p> <p><b>Property name:</b> _autoDeploymentCheckFrequency</p>



## Integration Preferences

This chapter includes the main concepts, tasks, and reference information for SiteScope Integration Preferences.

### **This chapter includes:**

#### **Concepts**

- ▶ Integration Preferences Overview on page 1416

#### **Tasks**

- ▶ Configure SiteScope-HP Business Availability Center Integration Preferences for Inaccessible Profiles on page 1423

#### **Reference**

- ▶ XML Tag Reference for Generic Data Integration on page 1426
- ▶ Integration Preferences User Interface on page 1429

## Integration Preferences Overview

Using the Integration Preferences interface, you can create integration instances, enabling SiteScope to report monitoring data to the following applications:

- ▶ **HP Business Availability Center**
  - ▶ For details on understanding the integration, see “Integrating with HP Business Availability Center” on page 149
  - ▶ For details on the integration preferences, see “HP Business Availability Center Integration Preferences” on page 1417.
  - ▶ For details on the user interface, see “New/Edit BAC Integration Dialog Box” on page 1432.
- ▶ **HP Diagnostics**
  - ▶ For details on understanding the integration, see “Diagnostics Integration Overview” on page 1420.
  - ▶ For details on the user interface, see “New/Edit Diagnostics Integration Dialog Box” on page 1442.
- ▶ **Generic data applications.**
  - ▶ For details on understanding the integration, see “Generic Data Integration Overview” on page 1421.
  - ▶ For details on the user interface, see “New/Edit Data Integration Dialog Box” on page 1437.

For details on configuring integration preference values, see “Integration Preferences User Interface” on page 1429.



## **HP Business Availability Center Integration Preferences**

To enable logging of SiteScope monitor data to Business Availability Center, the SiteScope must be configured as a data collector for Business Availability Center. This involves adding a SiteScope to the System Availability Management Administration page in the Business Availability Center. Once the SiteScope is added and a connection is established, a BAC Integration Preference appears in the Integration Preferences page that includes the relevant configurations as entered in the New SiteScope Page in System Availability Management Administration.

You use the Integration preference to:

- ▶ Modify the available integration settings.
- ▶ Disable logging all data to Business Availability Center. This includes topology reporting.
- ▶ Create an integration for an empty SiteScope profile. If when adding the SiteScope to System Availability Management Administration, the SiteScope was not accessible to Business Availability Center (for example, when working in HP Software-as-a-Service), you add a SiteScope with an **Inaccessible profile** to System Availability Management Administration. You then configure the connection and the integration in the Integration Preferences. For details on this task, see “Configure SiteScope-HP Business Availability Center Integration Preferences for Inaccessible Profiles” on page 1423.

If the HP Business Availability Center Server to which you are connecting is on a different machine than the HP Business Availability Center Server that SiteScope reports data, you must provide connection information for both servers under the **Main Settings** in SiteScope’s Integration Preferences, or in the **Distributed Settings** in System Availability Management Administration’s New SiteScope Page.

This section contains the following topics:

- ▶ “Using SSL for SiteScope-HP Business Availability Center Communication” on page 1418
- ▶ “Changing the Gateway Server to Which SiteScope Sends Data” on page 1419
- ▶ “Troubleshooting and Limitations” on page 1419
- ▶ “Configuring Integration Preferences” on page 1419

### **Using SSL for SiteScope-HP Business Availability Center Communication**

You can use Secure Sockets Layer (SSL) to transmit data from SiteScope to the Business Availability Center server. If you have installed a certificate signed by a root Certificate Authority on the Business Availability Center server, no additional setup is required on the SiteScope server. If you are using a self-signed certificate on the HP Business Availability Center server and want to use that certificate for secure communication with SiteScope, you must perform the steps as described in “Use SSL for SiteScope-HP Business Availability Center Communication” on page 1424.

---

#### **Note:**

- ▶ You only need to specify these settings if the certificate installed on the Business Availability Center machine is not signed by a root Certificate Authority (CA). For example, if you are using a certificate signed by a Certificate Authority such as Verisign, you do not need to change these settings.
  - ▶ You can import the self-signed certificate into the same keystore file used for other SiteScope monitors but that is not required. You can create a separate keystore for the Business Availability Center server certificate.
-

## Changing the Gateway Server to Which SiteScope Sends Data

You can change the Gateway Server to which a SiteScope reports its data. Generally, this is applicable only if you are working with an HP Business Availability Center deployment with components installed on more than one server. You make this change by entering the required Gateway Server name or IP address in the **Business Availability Center server machine name/IP address** box in the Integration Preferences page. You must also update the SiteScope settings with the **Gateway Server** name in System Availability Management Administration.

---

**Note:** This function can only be used for changing the Gateway Server for a SiteScope that is already registered with a given HP Business Availability Center installation. It cannot be used to add a new SiteScope, or to connect a SiteScope to a different HP Business Availability Center system.

---

## Troubleshooting and Limitations

For information about troubleshooting reporting data to HP Business Availability Center, see “Troubleshooting and Limitations” on page 170.

## Configuring Integration Preferences

For details on configuring these preferences, see “Integration Preferences User Interface” on page 1429.

## **Diagnostics Integration Overview**

SiteScope forwards data to HP Diagnostics enabling you to see a more complete view of the application servers that are monitored by Diagnostics. The data can provide insight into the infrastructure components onto which the application servers are deployed.

For example, integrating data from the SNMP by MIB monitor can help determine problems with the infrastructure on which the application server runs.

SiteScope forwards data on groups, monitors, and measurements. HP Diagnostics can read the data sent from SiteScope and present the data in its reports and graphs.

### **Units of Measurements in Diagnostics**

SiteScope generates a file `<SiteScope root directory>/conf/integration/data_integration_uom.xml` that controls the mappings of SiteScope monitors to Diagnostics metrics and the units of measurement used for the metrics. Diagnostics accepts data from SiteScope only if the data is associated with a unit of measurement that Diagnostics can recognize. SiteScope units are captured from the monitored source and may need to be mapped to the appropriate Diagnostics unit of measurement. The units of

measurements used by SiteScope monitors vary, depending on the type of data being monitored. For example, the unit of measurement used for the CPU monitor is a percentage and the unit of measurement used for the Disk Space monitor is number of bytes. It is therefore recommended that you modify the xml file as needed so that Diagnostics recognizes the unit of measurement to use for the monitor data coming from SiteScope.

When new monitors are added to the SiteScope that report data to Diagnostics, it is recommended that you edit the Diagnostics Integration Preference and click the **Generate UOM XML** button. SiteScope generates a list of currently deployed monitors and their corresponding metrics. This list merges with the `<SiteScope root directory>/conf/integration/data_integration_uom.xml` file and updates only those values in the xml file that were not manually changed. If any values were manually changed in the xml file, those values are not updated and are preserved. This merge of information on units of measurements occurs when you click this button and upon each SiteScope restart (by default every 24 hours).

For details on the user interface, see “New/Edit Diagnostics Integration Dialog Box” on page 1442.



## **Generic Data Integration Overview**

This is a generic integration that can be used to forward data to another application. That application must be able to receive the XML files that SiteScope forwards. These files contain information regarding the status of the SiteScope’s groups, monitors, and measurements.

For a reference detailing the XML tags, elements, and attributes included in the integration file that SiteScope forwards to the receiving application, see “XML Tag Reference for Generic Data Integration” on page 1426.

This section contains the following topics:

- ▶ “Delivery via HTTP Request” on page 1422
- ▶ “Time Synchronization” on page 1422

## Delivery via HTTP Request

The receiving application must be enabled to receive the data from SiteScope. This means that the application should be able to receive the http request from the SiteScope server and to decipher the XML file when it arrives.

The http request includes the following header:

Content-Type: text/xml

If you selected to zip the contents of the XML file, then the http request includes the following header:

Content-Type: text/xml  
Content-Encoding: gzip

You select whether to zip the data in the New Data Integration dialog box when creating the integration in SiteScope. If you select to zip the data, your application must be able to unzip the file SiteScope sends.

## Time Synchronization

You can synchronize the time of the SiteScope server with your application's server by enabling SiteScope to forward a separate time synchronization XML file. This file is sent in the same way as the data XML and at an interval you select in the **Time synchronization interval** field in the New Data Integration dialog box when creating the integration in SiteScope. If you enter a value in this field, SiteScope forward the date stamp of its server to the application receiving its data at the interval specified. For details on this option, see "Time synchronization interval (minutes)" on page 1438. For details on the contents of this XML file, see "Time Synchronization XML" on page 1429.

For details on the user interface, see "New/Edit Data Integration Dialog Box" on page 1437.

## **Configure SiteScope-HP Business Availability Center Integration Preferences for Inaccessible Profiles**

This task describes the steps involved in configuring SiteScope as a data collector for Business Availability Center when the SiteScope is inaccessible to the Business Availability Center, for example when working in HP Software-as-a-Service.

This task includes the following steps:

- “Add a SiteScope Profile to HP Business Availability Center” on page 1424
- “Specify Connection Parameters to HP Business Availability Center Servers” on page 1424
- “Configure SSL for SiteScope-HP Business Availability Center Communication” on page 1424

### **1 Add a SiteScope Profile to HP Business Availability Center**

In Business Availability Center, create an empty profile for the SiteScope in System Availability Management Administration's New SiteScope page by selecting **Inaccessible profile**. For details on the user interface, see "New SiteScope Page" on page 133.

### **2 Specify Connection Parameters to HP Business Availability Center Servers**

In SiteScope, add a new BAC Integration Preference to the Integration Preferences. Enter the values for the Business Availability Center integration. When adding the integration, click the **Get Available Profile** button and select the empty profile you created in Business Availability Center. For details on the user interface, see "New/Edit BAC Integration Dialog Box" on page 1432.

### **3 Configure SSL for SiteScope-HP Business Availability Center Communication**

If you are using a self-signed certificate on the HP Business Availability Center server and want to use that certificate for secure communication with SiteScope, you must import the certificate from the Business Availability Center server to the keystore on the SiteScope server and add three entries to the **master.config** file on the SiteScope server.

For details on this task, see "Use SSL for SiteScope-HP Business Availability Center Communication" on page 1424.



### **Use SSL for SiteScope-HP Business Availability Center Communication**

This task describes the steps involved in enabling secure communication between SiteScope and HP Business Availability Center using a self-signed certificate.

**To use a self-signed certificate on the HP Business Availability Center server for secure communication with SiteScope:**

- 1** Obtain a copy of the self-signed certificate from the Business Availability Center server saved in a DER-encoded binary X.509 format. Normally, the certificate file has an extension of \*.cer.



- 2 Import the certificate into a keystore on the SiteScope server using the procedures described in “Configuring SiteScope to Use SSL” in the *HP SiteScope Deployment Guide* PDF.

---

**Note:** It is not necessary to create the certificate request file, because you already have a certificate.

---

- 3 Edit the **master.config** file in the **<SiteScope root directory>\groups** using a text editor. Add the following three entries with the data indicated:

```
_sslTrustedCertKeyStoreFile=<path>\<filename>
_sslTrustedCertKeyStorePassword=<keystorepassword>
_sslAcceptAllUntrustedCerts=<boolean>
```

For example, the entries added to the **master.config** file may be as follows:

```
_sslTrustedCertKeyStoreFile=c:\keystores\topaz.keystore
_sslTrustedCertKeyStorePassword=sUp3rS3cr3tP@ssw0RD
_sslAcceptAllUntrustedCerts=false
```

- 4 Save the changes to the file.
- 5 Restart the SiteScope server.

## XML Tag Reference for Generic Data Integration

When SiteScope forwards data for a generic data integrations, it does so using the XML files whose elements and attributes are described below. For details on creating the integration, see “Generic Data Integration Overview” on page 1421. For details on the user interface, see “New/Edit Data Integration Dialog Box” on page 1437.

This section includes:

- ▶ “Data XML Elements and Attributes Table” on page 1426
- ▶ “Time Synchronization XML” on page 1429

### Data XML Elements and Attributes Table

Parent Element	Description of Element	Attribute	Description
performance Monitors	The parent element of the XML. Includes all group elements within it.	collectorHost	SiteScope host
		collector	Application collecting the data, which is always SiteScope
group	Represents the SiteScope group and is parent element to group and monitor element	name	Group name as defined by the user
		desc (optional)	Group description if entered for the group
		previousName (optional)	Previous name of the group if existed

Parent Element	Description of Element	Attribute	Description
monitor	Represents the SiteScope monitor and parent element to the counter element	type	Monitor type (as displayed in New Monitor dialog box)
		name	Monitor name as defined by the user
		target	Remote server being monitored
		time	Time of the measurement
		quality	Status as determined by the monitor's thresholds <b>Possible values:</b> <ul style="list-style-type: none"> <li>➤ 0 - no data (no thresholds defined)</li> <li>➤ 1 - informational (good)</li> <li>➤ 2 - warning</li> <li>➤ 3 - critical</li> </ul>
		previousName (optional)	Previous name of the monitor if existed
		desc (optional)	Monitor description if entered for the monitor
		statusDesc (optional)	Represents monitor's status string that is included only if the <b>Include additional data</b> is selected when creating the integration. For details on this option, see "Include additional data" on page 1439.

Parent Element	Description of Element	Attribute	Description
counter	Represents the measurements gathered by the monitor	name	Counter name
		value	Counter value
		quality	Status of the counter as determined by the counter's threshold  <b>Possible values:</b> <ul style="list-style-type: none"> <li>➤ 0 - no data (no thresholds defined)</li> <li>➤ 1 - informational (good)</li> <li>➤ 2 - warning</li> <li>➤ 3 - critical</li> </ul>
		desc (optional)	Monitor description if entered for the monitor
		status (optional)	If this attribute appears with a value of 0, the counter is not available. This attribute is not sent by SiteScope and not included in the XML if the counter is available.  <b>Possible value:</b> 0 - counter not available
		units (optional)	Units of measurements for the counter if relevant

## Time Synchronization XML






If you enter a value in the **Time synchronization interval** field when creating the data integration, SiteScope sends this XML to synchronize the time of the SiteScope server with that of the receiving application.

Parent Element	Description of Element	Attribute	Attribute Description
performanceMonitors	The parent element of the XML	collectorHost	SiteScope host
		collector	Application collecting the data, which is always SiteScope
timeStamp	Provides the time of the SiteScope server	timestamp	Time stamp, calculated as the seconds since January 1st 1970


## Integration Preferences User Interface

<b>Description</b>	Use to configure SiteScope as a data collector for HP Business Availability Center, Diagnostics, or other applications. If SiteScope has been configured as a data collector for HP Operations Manager, you can also view and modify some of the integration settings. <b>To access:</b> Select <b>Preferences</b> context > <b>Integration Preferences</b>
<b>Important Information</b>	Only an administrator in SiteScope, or a user granted <b>Edit integration preferences</b> permissions can create or make changes to Integration Preferences.
<b>Included in Tasks</b>	“Configure SiteScope-HP Business Availability Center Integration Preferences for Inaccessible Profiles” on page 1423
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Integration Preferences Overview” on page 1416</li> <li>➤ “Troubleshooting and Limitations” on page 170</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Click the <b>New Integration</b> button to create a new integration in SiteScope. For details on the user interface, see “Integration Preference Type Dialog Box” on page 1431.</p>
	<p>Click the <b>Edit Integration</b> button to edit an existing integration in SiteScope. The Edit Integration dialog box opens according to the integration type selected.</p> <ul style="list-style-type: none"> <li>▶ For details on the BAC Integration user interface, see “New/Edit BAC Integration Dialog Box” on page 1432.</li> <li>▶ For details on the Data Integration user interface, see “New/Edit Data Integration Dialog Box” on page 1437.</li> <li>▶ For details on the Diagnostics Integration user interface, see “New/Edit Diagnostics Integration Dialog Box” on page 1442.</li> </ul>
	<p>Click the <b>Delete Integration</b> button to delete the selected integration from Integration Preferences.</p>
	<p>Click the <b>Select All</b> button to select all listed integrations.</p>
	<p>Click the <b>Clear Selection</b> button to clear the selection.</p>
<p><b>Integration Name</b></p>	<p>The text name string assigned to the integration when you create a new Integration Preference.</p>
<p><b>Integration Description</b></p>	<p>A description of the integration that was assigned when creating or editing the Integration Preference.</p>



## Integration Preference Type Dialog Box

<b>Description</b>	Use to select the type of integration preference you want to configure. <b>To access:</b> Select <b>Preferences</b> context > <b>Integration Preferences</b> , and click the <b>New Integration</b>  button.
<b>Important Information</b>	Only an administrator in SiteScope, or a user granted <b>Edit integration preferences</b> permissions can create or make changes to Integration Preferences.
<b>Useful Links</b>	“Integration Preferences Overview” on page 1416

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Quick Search</b>	Enter an integration type in the <b>Quick Search</b> box.
<b>Select Integration Preference Name</b>	Select an integration preference type: <ul style="list-style-type: none"> <li>▶ <b>BAC Integration.</b> Use to configure SiteScope as a data collector for HP Business Availability Center. For details on the user interface, see “New/Edit BAC Integration Dialog Box” on page 1432.</li> <li>▶ <b>Data Integration.</b> Use to create a generic data integration. For details on the user interface, see “New/Edit Data Integration Dialog Box” on page 1437.</li> <li>▶ <b>Diagnostics Integration.</b> Use to create a diagnostics integration. For details on the user interface, see “New/Edit Diagnostics Integration Dialog Box” on page 1442.</li> </ul>

## **New/Edit BAC Integration Dialog Box**

<b>Description</b>	<p>Enables you to modify Business Availability Center integration settings and to create a new Business Availability Center integration for a profile that was created in System Availability Management Administration but when the SiteScope was inaccessible.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Integration Preferences</b>. In the Integration Preferences page:</p> <ul style="list-style-type: none"> <li>▶ Click the <b>New Integration</b>  button and select <b>BAC Integration</b>, or</li> <li>▶ Select an existing BAC integration and click <b>Edit Integration</b> .</li> </ul>
<b>Important Information</b>	<p>Only an administrator in SiteScope, or a user granted <b>Edit integration preferences</b> permissions can create or make changes to Integration Preferences.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Integration Preferences Overview” on page 1416</li> <li>▶ “Integration Preferences User Interface” on page 1429</li> <li>▶ “Integration Preference Type Dialog Box” on page 1431</li> </ul>

### **BAC Integration Main Settings**

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Business Availability Center machine name/IP address</b>	<p>Enter the machine name or IP address of the Business Availability Center server to which you want this SiteScope to connect.</p> <p><b>Note:</b> This is a required field.</p>
<b>SiteScope agent machine location</b>	<p>Enter the location of the SiteScope server that you are connecting to Business Availability Center. You can specify any value that helps you identify the location of this specific SiteScope server.</p> <p><b>Note:</b> This is a required field.</p>



GUI Element	Description
<b>Business Availability Center user name</b>	Enter the username of a Business Availability Center administrator-level user.
<b>Business Availability Center user password</b>	Enter the password for the specified user.
<b>Disable all logging to Business Availability Center</b>	Select to stop SiteScope from sending data to Business Availability Center. This also disables all topology reporting. Clear the check box to enable logging again. <b>Default value:</b> Not selected
<profile>	The SiteScope profile in which Business Availability Center stores the data collected by SiteScope. <b>Note:</b> The profile must previously have been configured in Business Availability Center's System Availability Management Administration.
<b>Get Available Profile</b>	Click to display a list of available profiles. Use this button only if registering the SiteScope to an empty profile (Inaccessible Profile) that was created in System Availability Management Administration.

## Web Server Security Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Authentication user name</b>	If the Business Availability Center server is configured to use basic authentication, enter the username to access the server.

GUI Element	Description
<b>Authentication password</b>	If the Business Availability Center server is configured to use basic authentication, enter the password to access the server.
<b>Use SSL (HTTPS protocol)</b>	Select this option if the Business Availability Center server is configured to use the HTTPS protocol. <b>Default value:</b> Not selected

### Proxy Server Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Address</b>	Enter the proxy server address if applicable.
<b>User name</b>	Enter the username for the proxy server.
<b>Password</b>	Enter the password for the specified server.

## Topology Reporting Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):



GUI Element	Description
<b>Topology resynchronization time interval (days)</b>	<p>The number of days for SiteScope to synchronize topology data with Business Availability Center.</p> <p>The topology information SiteScope reports to Business Availability Center is synchronized when SiteScope restarts after this time interval has been reached. SiteScope restarts by default every 24 hours.</p> <p><b>Default value:</b> 7 days</p> <p><b>Note:</b> All topologies created by SiteScope and stored in CMDB are subjected to the aging process. To prevent aging, see “Aging of CIs in CMDB” on page 158.</p>
<b>Default topology probe domain</b>	<p>Enter the default domain of the SiteScope topology probe.</p> <p><b>Default value:</b> DefaultDomain</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p>
<b>Topology receiver port</b>	<p>Enter the topology receiver port used in Business Availability Center.</p> <p><b>Default value:</b> 80</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p>
<b>Topology receiver SSL port</b>	<p>Enter the topology receiver SSL port used in Business Availability Center.</p> <p><b>Default value:</b> 443</p> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p>

## BAC Preferences Available Operations

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Reset</b>	<p>This deletes all the Business Availability Center related settings from the SiteScope server and all SiteScope configurations are deleted from Business Availability Center. This also sends a message to the applicable Business Availability Center server to release the SiteScope agent from the corresponding profile.</p> <p><b>Note:</b> If you choose to reset the current settings, you have to create or use a different profile to reconnect SiteScope with Business Availability Center. Business Availability Center does not enable you to select a previously used connection profile.</p>
<b>Re-Synchronize</b>	<p>Forces SiteScope to resend all its configuration data to Business Availability Center. This data consists of all the group and monitor definitions. Re-synchronize also forces SiteScope to resend all topology data to Business Availability Center.</p>
<b>Hard Re-Synchronize</b>	<p>Forces SiteScope to resend all its configuration data and topology data to Business Availability Center. For configuration data, it also deletes the existing monitor and group data from Business Availability Center for this SiteScope profile.</p>

## **New/Edit Data Integration Dialog Box**

<b>Description</b>	<p>Enables you to create a new generic data integration or to edit an existing data integration. This can be used to forward SiteScope data to an application for which a direct integration does not exist.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Integration Preferences</b>. In the Integration Preferences page:</p> <ul style="list-style-type: none"> <li>▶ Click the <b>New Integration</b>  button and select <b>Data Integration</b>, or</li> <li>▶ Select an existing Data integration and click <b>Edit Integration</b> .</li> </ul>
<b>Important Information</b>	<p>Only an administrator in SiteScope, or a user granted <b>Edit integration preferences</b> permissions can create or make changes to Integration Preferences.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Integration Preferences Overview” on page 1416</li> <li>▶ “Generic Data Integration Overview” on page 1421</li> <li>▶ “Integration Preferences User Interface” on page 1429</li> <li>▶ “Integration Preference Type Dialog Box” on page 1431</li> </ul>

### **General Settings**

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Name</b>	<p>Enter a name by which to identify this integration in the SiteScope interface.</p> <p><b>Note:</b> This is a required field.</p>
<b>Description</b>	<p>Optionally, enter a description of the integration. This could include information on the application receiving the data from SiteScope. This description appears only in the Integration Preferences page in SiteScope.</p>

## Data Integration Preferences Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Receiver URL</b>	<p>The URL of the application server to receive the SiteScope data. This must be a full URL including server, port, and path.</p> <p>If secure connection (SSL), then enter https.</p> <p><b>Syntax:</b> http or https://&lt;fully qualified domain name of the receiving server&gt;:&lt;port number receiving data&gt;/&lt;path&gt;</p>
<b>Encoding</b>	<p>Encoding used by the receiving application.</p> <p><b>Default value:</b> UTF-8</p>
<b>Reporting interval (seconds)</b>	<p>Time in seconds between when SiteScope finishes sending data to the next period SiteScope begins sending data.</p> <p><b>Default value:</b> 60 seconds</p>
<b>Time synchronization interval (minutes)</b>	<p>To synchronize between the time of the SiteScope server and the server receiving SiteScope data, SiteScope can periodically report the time that is registered on its server. The receiving server can then synchronize the time of the data samples coming from SiteScope with the time on its own server so that there is no discrepancy between the time of the SiteScope data and the application's own data.</p> <p>Select in minutes how often you want SiteScope to report to the time of the SiteScope server to the server receiving SiteScope data.</p> <p><b>Default value:</b> 10 minutes</p>

GUI Element	Description
<b>GZIP compression</b>	<p>If selected, SiteScope compresses the sample data sent to the receiving server. If the data is compressed, then performance is improved because the time to send data is reduced. Select or clear this field depending on the amount of data being sent and whether the receiving application can handle compressed data.</p> <p><b>Default value:</b> Not selected</p>
<b>Include additional data</b>	<p>If cleared, SiteScope reports the status of the following SiteScope objects:</p> <ul style="list-style-type: none"> <li>▶ groups</li> <li>▶ monitors</li> <li>▶ counters</li> </ul> <p>If selected, the status of these objects are reported along with the status string, which includes the descriptions of each object. It is recommended not to include this data as it slows performance and the status string repeats the status data sent by default.</p> <p><b>Default value:</b> Not selected</p>
<b>Error on redirect</b>	<p>If selected, SiteScope returns an error status if the target URL is redirected.</p> <p><b>Default value:</b> Not selected</p>
<b>Request timeout (seconds)</b>	<p>Sets the timeout in seconds until a connection is established with the server. A value of zero means there is no timeout used.</p> <p><b>Default value:</b> 120</p>
<b>Connection timeout (seconds)</b>	<p>Sets the socket timeout in seconds to wait for data. A timeout value of zero means there is no timeout used.</p> <p><b>Default value:</b> 120</p>
<b>Number of retries</b>	<p>The number of times SiteScope attempts to establish a connection.</p> <p><b>Default value:</b> 3</p>

GUI Element	Description
<b>Authentication when requested</b>	If selected, enables SiteScope to send user name and password credentials if requested. If cleared, SiteScope does not forward credentials. <b>Default value:</b> Selected
<b>Disable integration</b>	If selected, SiteScope does not forward data to the server. The integration preference setting remains. Use when temporarily disabling the integration. <b>Default value:</b> Not selected

### Web Server Security Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Authentication user name</b>	If the server is configured to use basic authentication, enter the username to access the server.
<b>Authentication password</b>	If the server is configured to use basic authentication, enter the password to access the server.
<b>Use SSL (HTTPS protocol)</b>	Select this option if the server is configured to use the HTTPS protocol. <b>Default value:</b> Not selected

### Proxy Server Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Address</b>	Enter the proxy server address if applicable.
<b>User name</b>	Enter the username for the proxy server.
<b>Password</b>	Enter the password for the specified server.





## Reporting Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>SiteScope uses the tag selected here to determine what data is forwarded to the receiving application. You must select at least one tag for each integration. That same tag must be selected for the groups, subgroups, and monitors whose data you want forwarded to the receiving application.</p> <p>When selecting an integration tag for an object, the tag propagates to that object's children. If you tag a group with this Integration tag, all its subgroups and monitors report their status to the receiving application.</p> <p><b>Example:</b> Create a tag called <code>Integration1</code> and select it here. For each group and/or monitor whose status you want to report to the receiving application, select this tag under the <b>Search/Filter Tags</b> setting for the object.</p> <p><b>Note:</b> You can select multiple tags for each integration preference. You can select multiple Integration tags for the objects to be reported.</p>
<b>Add Tag</b>	<p>Click to open the New Tag dialog box and create a new tag.</p> <p><b>Tip:</b> Use the word <code>Integration</code> when creating an Integration tag. Because the Integration tags appear along with all other Search/Filter tags created for the SiteScope, this helps you identify which tag to select for enabling a group or monitor for the integration.</p> <p>For details on the New Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>

## **New/Edit Diagnostics Integration Dialog Box**

<b>Description</b>	<p>Enables you to create a new integration with HP Diagnostics or to edit an existing Diagnostics integration.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Integration</b>. In the Integration Preferences page:</p> <ul style="list-style-type: none"> <li>➤ Click the <b>New Integration</b>  button and select <b>Diagnostics Integration</b>, or</li> <li>➤ Select an existing Diagnostics integration and click <b>Edit Integration</b> .</li> </ul>
<b>Important Information</b>	<p>Only an administrator in SiteScope, or a user granted <b>Edit integration preferences</b> permissions can create or make changes to Integration Preferences.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Diagnostics Integration Overview” on page 1420</li> <li>➤ “Integration Preferences User Interface” on page 1429</li> <li>➤ “Integration Preference Type Dialog Box” on page 1431</li> </ul>

### **General Settings**

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Name</b>	<p>Enter a name by which to identify this integration in the SiteScope interface.</p> <p><b>Note:</b> This is a required field.</p>
<b>Description</b>	<p>Optionally, enter a description of the integration. This could include information on the Diagnostics server receiving the data from SiteScope. This description appears only in the Integration Preferences page in SiteScope.</p>

## Diagnostics Integration Preferences Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Receiver URL</b>	<p>The URL of the Diagnostics server to receive the SiteScope data. This must be a full URL including server, port where diagnostics receives data, and path. The path must always include <b>/metricdata/siteScopeData</b>.</p> <p>If secure connection (SSL), then enter https.</p> <p><b>Syntax:</b> http or https://&lt;fully qualified domain name of the receiving server&gt;:&lt;port number receiving data&gt;/<b>metricdata/siteScopeData</b></p> <p><b>Example:</b> http://DiagnosticsServer1.hp.net:2006/metricdata/siteScopeData</p>
<b>Encoding</b>	<p>Encoding used by the Diagnostics application.</p> <p><b>Default value:</b> UTF-8</p>
<b>Reporting interval (seconds)</b>	<p>Time in seconds between when SiteScope finishes sending data to the Diagnostics server to the next period SiteScope sends data. This time interval can prevent communication delays between the servers as it is an interval of time when no data is sent.</p> <p><b>Default value:</b> 60</p>
<b>Time synchronization interval (minutes)</b>	<p>To synchronize between the time of the SiteScope server and the Diagnostics server, SiteScope periodically reports the time that is registered on its server. Diagnostics then synchronizes the time of the data samples coming from SiteScope with the time on its own server so that there is no discrepancy between the time of the SiteScope data and the Diagnostics data.</p> <p>Select in minutes how often you want SiteScope to report to Diagnostics the time of the SiteScope server.</p> <p><b>Default value:</b> 10 minutes</p>

GUI Element	Description
<b>GZIP compression</b>	<p>If selected, SiteScope compresses the sample data sent to the Diagnostics server. If the data is compressed, then performance is improved because the time to send data is reduced. The Diagnostics application can handle compressed data. Select or clear this field depending on the amount of data being sent.</p> <p><b>Default value:</b> Selected</p>
<b>Include additional data</b>	<p>If cleared, SiteScope reports the status of the following SiteScope objects:</p> <ul style="list-style-type: none"> <li>▶ groups</li> <li>▶ monitors</li> <li>▶ counters</li> </ul> <p>If selected, the status of these objects are reported along with the status string, which includes the descriptions of each object. It is recommended not to include this data as it slows performance and the status string repeats the status data sent by default.</p> <p><b>Default value:</b> Not selected</p>
<b>Error on redirect</b>	<p>If selected, SiteScope returns an error status if the target URL is redirected.</p> <p><b>Default value:</b> Not selected</p>
<b>Request timeout (seconds)</b>	<p>Sets the socket timeout in seconds which is the timeout for waiting for data. A timeout value of zero is interpreted as an infinite timeout.</p> <p><b>Default value:</b> 120</p>
<b>Connection timeout (seconds)</b>	<p>Sets the timeout until a connection is established. A value of zero means the timeout is not used.</p> <p><b>Default value:</b> 120</p>
<b>Number of retries</b>	<p>The number of times SiteScope attempts to establish a connection.</p> <p><b>Default value:</b> 3</p>

GUI Element	Description
<b>Authentication when requested</b>	If selected, enables SiteScope to send user name and password credentials if requested. If cleared, SiteScope does not forward credentials. <b>Default value:</b> Selected
<b>Disable integration</b>	If selected, SiteScope does not forward data to the Diagnostics server. The integration preference settings remain. Use when temporarily disabling the integration. <b>Default value:</b> Not selected
<b>Generate UOM XML</b>	Click this button to generate a units of measurement xml file to merge with the <SiteScope root directory>/conf/integration/data_integration_uom.xml file. This file enables Diagnostics to read the SiteScope data and apply the appropriate unit of measurement to the data. It is recommended that you click this button when a monitor instance is added that reports data to Diagnostics. If any values were manually changed in the data_integration_uom.xml file, those values remain and are not updated by this merge file. This merge file is also generated and updates the xml file upon every SiteScope restart (by default every 24 hours). For details, see “Units of Measurements in Diagnostics” on page 1420.

### Web Server Security Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Authentication user name</b>	If the server is configured to use basic authentication, enter the username to access the server.
<b>Authentication password</b>	If the server is configured to use basic authentication, enter the password to access the server.

## Proxy Server Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Address	Enter the proxy server address if applicable.
User name	Enter the username for the proxy server.
Password	Enter the password for the specified server.

## Reporting Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>SiteScope uses the tag selected here to determine what data is forwarded to Diagnostics. You can select more than one tag for each integration. The tag must be selected for the groups, subgroups, and monitors whose data you want forwarded to Diagnostics.</p> <p>When selecting an Integration tag for an object, the tag propagates to that object's children. If you tag a group with this Integration tag, all its subgroups and monitors report their status to Diagnostics.</p> <p><b>Example:</b> Create a tag called <code>Diagnostics_Integration1</code> and select it here. For each group and/or monitor whose status you want to report to Diagnostics, select this tag under the <b>Search/Filter Tags</b> setting.</p>
<b>Add Tag</b>	<p>Click to open the New Tag dialog box and create a new tag.</p> <p><b>Tip:</b> Use the word <code>Integration</code> when creating an Integration tag. Because the Integration tags appear along with all other Search/Filter tags created for the SiteScope, this helps you identify which tag to select for enabling a group or monitor for the integration.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>





# 120

---

## Log Preferences

This chapter includes the main concepts and reference information for SiteScope Log Preferences.

### **This chapter includes:**

#### Concepts

- ▶ Log Preferences Overview on page 1449

#### Reference

- ▶ SiteScope Log Database Table Structure on page 1450
- ▶ Log Preferences User Interface on page 1452

**Troubleshooting and Limitations** on page 1455

### **Log Preferences Overview**

Log Preferences enable you to select how much monitor data is accumulated and maintained on the SiteScope server. It also configures SiteScope to export monitor data to an external database.

By default, SiteScope saves monitor results, alert data, error data, and other readings returned by monitors into log files. For monitor data results, a date-coded log file is created for each 24-hour period of monitoring. This data is stored as tab delimited text. SiteScope uses the log files to create management reports on system availability and performance over time.

Storing data logs can become a problem over time. However, you can limit how much log information SiteScope saves to the local file system by setting the number of days to maintain log files or by setting a maximum data log file size. You can also send monitoring data to an external database application. This helps reduce the data storage capacity required on the SiteScope server and makes the monitoring data available to other reporting tools.

---

**Note:** To create SiteScope Management Reports the monitoring log information for the desired time period of the report must be available on the SiteScope server file system. For details on creating management reports, see “Management Report” on page 2072.

---

For details on configuring these preferences, see “Log Preferences User Interface” on page 1452.

## SiteScope Log Database Table Structure

When database login is enabled, monitor data is contained in a single table called **SiteScopeLog**. The first nine fields of each database record are the same for all monitors. The next ten fields contain different measurements depending on the kind of monitor supplying the data. All the fields in the table use the VARCHAR(255) data type. A description of the fields in the log database record are shown in the table below along with their default field names:

Field Name	Example Data	Description
datex	1999-01-20 11:54:54	The first field contains the date that the monitor ran.
serverName	demo.sitescope.com	The second field contains the name of the server where SiteScope is running.

Field Name	Example Data	Description
class	URLMonitor	The third field contains the type of the monitor.
sample	23	The fourth field contains the sample number of this monitor.
category	good	The fifth field contains the category name of the monitor.
groupName	URLs	The sixth field contains the group name of the monitor.
monitorName	Home Page	The seventh field contains the name of the monitor.
status	1.01 seconds	The eighth field contains the status of the monitor.
monitorID	10	The ninth field contains the ID of the monitor.
value1, value2, ... value10	(variable)	The tenth through nineteenth fields contain the monitor specific data as described in the Log Columns page. The first variable field (value1) corresponds to the value listed as column 7 in the log files.

The SQL statement that is used for database logging can be changed by editing the parameter `_logJdbcInsertSiteScopeLog=` in the `<SiteScope root directory>\groups\master.config` file. A stored procedure can be called by replacing the insert statement with a call statement. For example, call `logit(?,?,?)` would call the stored procedure named `logit` passing it the first three parameters.

## Log Preferences User Interface

<b>Description</b>	<p>Effective system availability monitoring requires that monitoring data be recorded and stored for a required interval of time. SiteScope Log Preferences controls the accumulation and storage of monitor data.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Log Preferences</b></p>
<b>Important Information</b>	<p>Only an administrator in SiteScope, or a user granted <b>Edit log preferences</b> permissions can create or make changes to Log Preferences.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Log Preferences Overview” on page 1449</li> <li>▶ “SiteScope Log Database Table Structure” on page 1450</li> <li>▶ “Troubleshooting and Limitations” on page 1455</li> </ul>

### SiteScope Log File Preferences

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Daily logs to keep</b>	<p>Enter the number of days of monitoring data to keep. Once a day, SiteScope deletes any logs older than the specified number of days.</p> <p><b>Default value:</b> 40</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ The last two logs (today's and yesterday's) are always preserved, regardless of the number of logs or maximum log size specified.</li> <li>▶ Keeping monitor data logs for long periods can cause a data storage problem for the SiteScope server depending on the total number of monitors configured and how often the monitors run per day. You should monitor the size of the log files in the <b>&lt;SiteScope root directory&gt;\logs</b> directory to estimate the data accumulation rate, and adjust this setting or server resources as necessary.</li> </ul>

GUI Element	Description
<b>Maximum size of logs (MB)</b>	<p>Enter the maximum size allowed for all monitoring logs. Once a day, SiteScope checks the total size of all monitoring logs and removes any old logs that are over the maximum size.</p> <p><b>Default value:</b> 0 (the log size is not checked)</p>

### Database Logging Preferences

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Database connection URL</b>	<p>To enable Database logging, enter a URL to a Database Connection. The easiest way to create a database connection is to use ODBC to create a named connection to a database.</p> <p><b>Example:</b> First use the ODBC control panel to create a connection called SiteScopeLog. Then, enter <code>jdbc:odbc:SiteScopeLog</code> as the connection URL.</p> <p><b>Note for using Windows Authentication:</b> If you want to access the database using Windows authentication, enter <code>jdbc:mercury:sqlserver://&lt;server name or IP address&gt;:1433;DatabaseName=&lt;database name&gt;;AuthenticationMethod=type2</code> as the connection URL, and <code>com.mercury.jdbc.sqlserver.SQLServerDriver</code> as your database driver. Leave the <b>Database user name</b> and <b>Database password</b> boxes empty, since the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.</p>

GUI Element	Description
<b>Database driver</b>	<p>Specify the database driver SiteScope should use to connect to the database. The driver should be a JDBC driver. To have SiteScope use another driver the driver must also be installed in the <b>&lt;SiteScope root directory&gt;\WEB-INF\lib</b> directory and the path and filename must be entered in this box.</p> <p><b>Default value:</b> sun.jdbc.odbc.JdbcOdbcDriver</p>
<b>Database user name</b>	<p>Enter the user name used to log in to the database. If using Microsoft SQL server, leave this blank and choose Windows Authentication when setting up the ODBC connection. With Windows Authentication, you cannot specify a user name as SiteScope connects using the login account of the SiteScope service.</p> <p><b>Note for using Windows Authentication:</b> The user that is running SiteScope must have access to the database to which you are connecting. If SiteScope is running under a Local Systems Account, it attempts to connect using the name of the server.</p>
<b>Database password</b>	<p>Enter a password to login to the database. If using Microsoft SQL server, leave this blank and choose Windows Authentication when creating the ODBC connection. With Windows Authentication, you cannot specify a password as SiteScope connects using the login account of the SiteScope service.</p>
<b>Backup database connection URL</b>	<p>Enter a URL to a backup database. Use this option to provide failover of SiteScope database logging if the primary database becomes unavailable.</p> <p><b>Note:</b> The same database table definition, database driver, user name, and password are applied to both database connections.</p> <p>After saving changes to the Database preferences, stop and restart the SiteScope service for the changes take effect.</p>

## Troubleshooting and Limitations

When Database logging is active and working correctly, you should see a table called **SiteScopeLog** in your database and a record added to the table every time a monitor runs. The data is sent to the database as a single table in a flat-file format.

If the **SiteScopeLog** table is not created or is empty, check the `<SiteScope root directory>\logs\RunMonitor.log` and `<SiteScope root directory>\logs\Error.log` files for log messages starting with "jdbc" or "odbc". When Database logging is working correctly, you should see a set of messages in **RunMonitor.log** that looks like this:

```
jdbc log, reconnect seconds=600
jdbc log, loading, driver=sun.jdbc.odbc.JdbcOdbcDriver
jdbc log, connecting, url=jdbc:odbc:SiteScopeLog,
jdbc log, logged in
jdbc log, checking log table
jdbc log, created log table
jdbc log, prepare insert, 19, INSERT INTO SiteScopeLog...
jdbc log, connected
```

If these entries do not appear in the log file there is a problem with the database interface or configuration of the database connection. You should also check the Database Connection URL you entered. This parameter is case sensitive. Check the spelling and letter case of the connection URL and make sure there are no leading or trailing spaces present in the text box.

You can also check the HP Software Self-solve knowledge base (<http://h20230.www2.hp.com/selfsolve/documents>) for other information relating to database logging. To enter the knowledge base, you must log in with your HP Passport ID.





# 121

---

## Failover Preferences

This chapter includes the main concepts and reference information for SiteScope Failover preferences.

### **This chapter includes:**

#### Concepts

- ▶ Failover Preferences Overview on page 1457

#### Reference

- ▶ Failover Preferences User Interface on page 1458

### **Failover Preferences Overview**

---

**Note:** Failover Preferences are available only to users accessing SiteScope Failover that have a SiteScope Failover license.

---

When using SiteScope Failover, a special version of SiteScope that includes automated mirroring and failover functionality, you can use Failover Preferences to indicate a primary SiteScope to be mirrored and set how often the configurations should be mirrored to the failover SiteScope installation. For information on using SiteScope Failover, refer to the *SiteScope Failover Guide* PDF.

For details on configuring these preferences, see “Failover Preferences User Interface” on page 1458.

## Failover Preferences User Interface

<b>Description</b>	<p>SiteScope Failover is a special version of SiteScope that includes automated mirroring and failover functionality. It enables you to implement failover capability for infrastructure monitoring by provisioning for backups, redundant, and failover mechanisms. Use the Failover Preferences to indicate a primary SiteScope to be mirrored and set how often the configurations should be mirrored to the failover SiteScope installation.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Failover Preferences</b></p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The Failover Preferences are available only to users accessing SiteScope Failover that have a SiteScope Failover License.</li> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit failover preferences</b> permissions can create or make changes to Failover Preferences.</li> <li>▶ SiteScope Failover restarts itself after each mirroring operation.</li> <li>▶ For information on using SiteScope Failover, refer to the <i>SiteScope Failover Guide</i> PDF.</li> </ul>
<b>Useful Links</b>	“Failover Preferences Overview” on page 1457

### Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Host</b>	Enter the name or IP address of the server that you want this SiteScope Failover server to mirror configurations from.
<b>Port</b>	Enter the SiteScope port of the server that you want this SiteScope Failover server to mirror configurations from. <b>Default value:</b> 8888

GUI Element	Description
<b>Use SSL</b>	When this box is checked, the mirror server contacts the primary SiteScope server by using HTTPS. <b>Default value:</b> Not selected
<b>Admin login</b>	The login name used to access the administrator login account for the primary SiteScope instance. If no administrator login has been configured on the target machine, leave this box blank.
<b>Admin password</b>	The password used to access the administrator login account for the primary SiteScope instance. If no SiteScope administrator login has been configured on the primary SiteScope, leave this box blank.
<b>Mirror every (hours)</b>	The schedule for synchronizing (mirroring) configuration data to the failover SiteScope from the primary SiteScope. This is used to make sure that the SiteScope Failover configuration reflects updates and changes to the monitoring configuration on the primary SiteScope server. Values for this box should be between 1 to 23 hours. Enter values as whole numbers. <b>Default value:</b> 4 hours
<b>Last mirror time</b>	The time and date of the most recent mirroring operation.
<b>Next mirror time</b>	The time and date of the next scheduled mirroring operation.
<b>Mirror Configuration Now</b>	Click to mirror the primary SiteScope configuration data now.



# 122

---

## Email Preferences

This chapter includes the main concepts and reference information for SiteScope Email Preferences.

### **This chapter includes:**

#### Concepts

- ▶ Email Preferences Overview on page 1461

#### Reference

- ▶ Email Preferences User Interface on page 1462

### **Email Preferences Overview**

You use Email Preferences to configure the settings SiteScope needs to communicate with an external email server. These are the default settings that SiteScope uses to send alerts as email messages.






The Email Preferences page displays the defined custom Email Recipient profiles to send email alert messages to recipients. The Email Recipient profile can be associated with one or more Email alerts by editing the applicable alert definition.


For details on configuring these preferences, see “Email Preferences User Interface” on page 1462.

## Email Preferences User Interface



<b>Description</b>	<p>Email is the default media for sending event alerts when a problem has been detected by SiteScope (in addition to the visual icons and status messages displayed in the SiteScope interface). Use the Email Preferences to indicate the SMTP mail server, recipient addresses, and other settings that SiteScope should use when sending email alerts and other SiteScope messages.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Email Preferences</b></p>
<b>Important Information</b>	<p>Only an administrator in SiteScope, or a user granted <b>Edit email, pager and SNMP preferences</b> permissions can create or make changes to Email Preferences.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Email Preferences Overview” on page 1461</li> <li>▶ “New/Edit Email Recipient Dialog Box” on page 1464</li> <li>▶ “Email Preferences Default Settings Dialog Box” on page 1467</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click the <b>New Email Recipient</b> button to create a new Email Recipient profile. For details on the user interface, see “New/Edit Email Recipient Dialog Box” on page 1464.
	Click the <b>Edit Email Recipient</b> button to edit the Email Recipient profile. For details on the user interface, see “New/Edit Email Recipient Dialog Box” on page 1464.
	Click the <b>Delete Email Recipient</b> button to delete the selected Email Recipient profile from Email Preferences.
	Click the <b>Test Email Recipient</b> button to test that you can send a message to the Email address. Enter a message in the Email dialog box, and click <b>Test</b> .
	Click the <b>Select All</b> button to select all listed Email Recipient profiles.

GUI Element	Description
	Click the <b>Clear Selection</b> button to clear the selection.
<b>Default Settings</b>	<p>Click the arrow next to <b>Default Settings</b>, and select an option:</p> <ul style="list-style-type: none"> <li>▶ <b>Edit.</b> Opens the Email Preferences Default Settings dialog box which enables you to change the default settings displayed in the New Email Preferences dialog box. For details on the settings, see “Email Preferences Default Settings Dialog Box” on page 1467.</li> <li>▶ <b>Test.</b> Test that you can send an email to the selected addresses. Select the email recipients you want to test from the list of Available Recipients, or enter email addresses in the <b>Email addresses</b> box.</li> </ul>
<b>Name</b>	The text name string assigned to the setting profile when you create a new Email Recipient.
<b>Description</b>	A description of the setting profile that was assigned when creating or editing the profile.
<b>Email</b>	The email address to which the alert is to be sent.
<b>Enabled</b>	The enabled/disabled status of the email alert. If the status is <b>No</b> , email alerts are stopped from being sent to these email addresses.

 **New/Edit Email Recipient Dialog Box**

<p><b>Description</b></p>	<p>Enables you to create a new Email Recipient profile or edit an existing profile. SiteScope uses Email Recipient profiles for sending email alerts.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Email Preferences</b>. In the Email Preferences page:</p> <ul style="list-style-type: none"> <li>➤ Click the <b>New Email Recipient</b>  button, or</li> <li>➤ Select an existing Email Recipient profile and click <b>Edit Email Recipient</b> .</li> </ul>
<p><b>Important Information</b></p>	<p>Only an administrator in SiteScope, or a user granted <b>Edit email, pager and SNMP preferences</b> permissions can create or make changes to Email Preferences.</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ “Email Preferences Overview” on page 1461</li> <li>➤ “Email Preferences User Interface” on page 1462</li> <li>➤ “Email Preferences Default Settings Dialog Box” on page 1467</li> </ul>



## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Name</b>	Enter a text description for the Email Recipient profile definition. The name is used to identify the Email Recipient profile definition in the product display.
<b>Description</b>	<p>Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the &lt;BR&gt;, &lt;HR&gt;, and &lt;B&gt; tags to control display format and style.</p> <p><b>Note:</b> HTML code entered here is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> <li>▶ Tags: <b>script</b>, <b>object</b>, <b>param</b>, <b>frame</b>, <b>iframe</b>.</li> <li>▶ Any tag that contains an attribute starting with <b>on</b> is declined. For example, <b>onhover</b>.</li> <li>▶ Any attribute with <b>javascript</b> as its value.</li> </ul>
<b>Email to</b>	<p>The email addresses to which you want to send the alert.</p> <p><b>Example:</b> test@mycompany.com</p> <p>You can enter multiple email addresses by separating the email addresses with commas.</p> <p><b>Example:</b> test@mycompany.com, sysadmin@thiscompany.com</p>
<b>Disabled</b>	Stops email alerts from being sent to these email addresses. Use this option to temporarily disable a particular email without editing every alert that contains this email setting.

## Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Template</b>	Select a template from the drop-down list to define the email alert settings. Once a setting is defined, a single alert is sent to people and pagers. Use the <b>ShortMail</b> template for pagers.
<b>Schedule</b>	Use this option to specify when email settings should be enabled. You may select a more restricted schedule from the names schedules in the drop-down menu.  <b>Default value:</b> every day, all day

## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>&lt;Tag name and values&gt;</b>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.  For details on using tags, see “Working with Search/Filter Tags” on page 107.
<b>Add Tag</b>	Click to add a new keyword tag.  For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.

 **Email Preferences Default Settings Dialog Box**

<b>Description</b>	Enables you to configure the default Email Recipient settings. <b>To access:</b> Select <b>Preferences</b> context > <b>Email Preferences</b> . In the Email Preferences page, click the <b>Edit Default Settings</b> button.
<b>Important Information</b>	Only an administrator in SiteScope, or a user granted <b>Edit email, pager and SNMP preferences</b> permissions can create or make changes to Email Preferences.
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Email Preferences Overview” on page 1461</li> <li>▶ “Email Preferences User Interface” on page 1462</li> <li>▶ “New/Edit Email Recipient Dialog Box” on page 1464</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Email server domain name</b>	Enter the domain name of the SMTP mail server that SiteScope should use when sending email messages. <b>Example:</b> mail.thiscompany.com If you are unsure of your mail server's domain name, check with your System Administrator.
<b>Administrator email address</b>	Enter the email address to which SiteScope should send status messages. <b>Example:</b> sysadmin@thiscompany.com
<b>Daily status</b>	Select this option to have SiteScope send a brief daily status message to the administrator's email address. This email is scheduled to be generated at 7:07 AM every day. The subject of email sent includes <b>SiteScope daily status</b> . The email content includes the number of active monitors and groups, along with a URL link to the applicable SiteScope main page plus the version number of SiteScope installation.

GUI Element	Description
<b>SiteScope starts/restarts</b>	Select this option to have SiteScope send a brief message each time that SiteScope restarts. Normally, SiteScope automatically restarts itself once a day. Other restarts may be an indication of a monitor run problem. For more information, see “SiteScope Server Health” on page 1895.
<b>From email address</b>	Enter the email address used as the From Address for mail generated by SiteScope. Specifying an email address may make it easier to browse and sort email sent by SiteScope. If nothing is entered, the <b>From email address</b> stays the same as the address where the mail is sent from. <b>Example:</b> sitescope@mycompany.com <b>Note:</b> If the mail server being used required NTLM authentication (see below), the email address entered here must be a valid email address.
<b>Backup email server domain name</b>	Enter the domain name of the SMTP mail server that SiteScope should use whenever the primary mail server cannot be reached. If unsure of backup mail server's domain name, check with the System Administrator. <b>Example:</b> gateway.mycompany.com.
<b>Login</b>	Enter the username required by the SMTP server. This user name is used for both the primary and backup mail servers. <b>Note:</b> You must restart SiteScope if you change this setting.
<b>Password</b>	If the SMTP server you want SiteScope to use requires authentication, enter the password for username entered in the <b>Login</b> box. This password is used for both the primary and backup mail servers. <b>Note:</b> You must restart SiteScope if you change this setting.

GUI Element	Description
<b>NTLM authentication</b>	<p>Select an NTML authentication option from the drop-down list:</p> <ul style="list-style-type: none"> <li>▶ <b>none.</b> Select if the mail server does not require NTLM authentication.</li> <li>▶ <b>NTLMv1.</b> Select if the mail server requires authentication using NTLM version 1.</li> <li>▶ <b>NTLMv2.</b> Select if the mail server requires authentication using NTLM version</li> </ul> <p><b>Note:</b> You must restart SiteScope if you change this setting.</p> <p><b>Default value:</b> none</p>
<b>Timeout (seconds)</b>	<p>Enter an optional length of time to wait for a response from the SMTP server. If a response from the primary mail server is not received within the timeout period, SiteScope switches to use the backup mail server.</p> <p><b>Default value:</b> 60 seconds</p>



# 123

---

## Pager Preferences

This chapter includes the main concepts and reference information for SiteScope Pager Preferences.

**This chapter includes:**

**Concepts**

- ▶ Pager Preferences Overview on page 1472

**Reference**

- ▶ Pager Preferences User Interface on page 1473

## Pager Preferences Overview

You use Pager Preferences to configure the settings SiteScope needs to communicate with an external electronic paging service. These are the default settings that SiteScope uses to send alerts to an electronic pager.

The Pager Preferences page displays the defined custom Pager Recipient profiles. These profiles can be associated with one or more Pager alerts by editing the applicable alert definition.

You define Pager Recipient profiles in the New/Edit Pager Recipient page. The preferred pager connection option is **Modem to modem connection**. When this connection is used, SiteScope is able to verify that the message was sent successfully and can receive messages describing any communication problem. The other connection options generally send messages to automated voice response systems using touch tone dialing. The touch tone dialing method is limited to numeric messages and SiteScope cannot confirm that your paging service correctly received the message.




For details on configuring these preferences, see “Pager Preferences User Interface” on page 1473.






## Pager Preferences User Interface



<b>Description</b>	<p>Used to define pager recipient profiles and settings that SiteScope uses for sending Pager alerts to individuals or groups. Lists all the currently defined Pager Recipient profiles.</p> <ul style="list-style-type: none"> <li>▶ Sends an automated notification to system administrators who may not have immediate access to email.</li> <li>▶ Sends alert escalation or notifies support personnel who may be away from the office.</li> </ul> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Pager Preferences</b></p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit email, pager and SNMP preferences</b> permissions can create or make changes to Pager Preferences.</li> <li>▶ You cannot delete a Pager Recipient profile if it is referenced by an alert action. You must change the recipient in the alert before you can delete the profile.</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Pager Preferences Overview” on page 1472</li> <li>▶ “New/Edit Pager Recipient Dialog Box” on page 1475</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click the <b>New Pager Recipient</b> button to create a new Pager Recipient profile. For details on the user interface, see “New/Edit Pager Recipient Dialog Box” on page 1475.
	Click the <b>Edit Pager Recipient</b> button to edit the Pager Recipient profile. For details on the user interface, see “New/Edit Pager Recipient Dialog Box” on page 1475.
	Click the <b>Delete Pager Recipient</b> button to delete the selected Pager Recipient profile from Pager Preferences.

GUI Element	Description
	<p>Click the <b>Test Pager Recipient</b> button to test that you can send a message to the pager. Enter a message in the Test Pager dialog box, and click <b>Test</b>. You can enter a prefix that can be added to the pager message. If you are sending the message to a numeric pager, do not enter more than 32 digits.</p>
	<p>Click the <b>Select All</b> button to select all listed Pager Recipient profiles.</p>
	<p>Click the <b>Clear Selection</b> button to clear the selection.</p>
<p><b>Default Settings</b></p>	<p>Click the arrow next to <b>Default Settings</b>, and select an option:</p> <ul style="list-style-type: none"> <li>▶ <b>Edit.</b> Opens the Pager Preferences Default Settings dialog box which enables you to change the default settings displayed in the New Pager Preferences dialog box. For details on the settings, see “New/Edit Pager Recipient Dialog Box” on page 1475.</li> <li>▶ <b>Test.</b> Opens the Test Pager dialog box which enables you to test that you can send a message to the default pager. Enter a message in the <b>Message</b> box, and click <b>Test</b>. You can enter a prefix that can be added to the pager message. If you are sending the message to a numeric pager, do not enter more than 32 digits.</li> </ul>
<p><b>Name</b></p>	<p>The text name string assigned to the setting profile when you create a new pager recipient.</p>
<p><b>Description</b></p>	<p>A description of the setting profile that was assigned when creating or editing the profile.</p>

## **New/Edit Pager Recipient Dialog Box**

<b>Description</b>	<p>Enables you to create a new Pager Recipient profile or edit an existing profile. SiteScope uses Pager Recipient profiles for sending Pager alerts.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Pager Preferences</b>. In the Pager Preferences page:</p> <ul style="list-style-type: none"> <li>➤ Click the <b>New Pager Recipient</b>  button, or</li> <li>➤ Select an existing pager profile and click <b>Edit Pager Recipient</b> .</li> </ul>
<b>Important Information</b>	<p>Only an administrator in SiteScope, or a user granted <b>Edit email, pager and SNMP preferences</b> permissions can create or make changes to Pager Preferences.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Pager Preferences Overview” on page 1472</li> <li>➤ “Pager Preferences User Interface” on page 1473</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Name</b>	Enter the text name string assigned to the setting profile when you create a new pager recipient.
<b>Modem port</b>	<p>Select the communications port that the modem is connected to on the SiteScope server. For SiteScope on Solaris or Linux, enter the path and device name for the modem. On Microsoft Windows NT/2000 platforms, SiteScope uses COM port numbers for both RS-232C type serial ports as well as for USB modem ports.</p> <p>If you are using a USB type modem, select the COM port associated with the USB port to have SiteScope use the USB modem. To find the COM port number for the USB modem, use the <b>Settings &gt; Network and Dial-up Connections</b> menu. Right-click the desired modem, and then click <b>Properties</b>. The properties should show the COM port number that is associated to the modem.</p> <p><b>Default value:</b> COM1</p>

GUI Element	Description
<b>Connection speed (bit/sec)</b>	Select the modem speed used for connections to the paging service from the drop-down list. <b>Default value:</b> 1200 bit/sec
<b>Pager connection options</b>	Select an option for sending a message to your paging service: <ul style="list-style-type: none"> <li>▶ <b>Modem to modem connection (Preferred).</b> Select if you have an alphanumeric pager and use an alphanumeric paging service.</li> <li>▶ <b>Dial and enter message.</b> Select to dial a direct phone number to send a page.</li> <li>▶ <b>Dial, enter command and enter message.</b> Select if you have a direct number, but need to enter a command before sending a page.</li> <li>▶ <b>Custom modem connection.</b> Select if your paging company does not use any of the previous connection choices.</li> </ul> <p>For details of the information required for the selected option, see the table below.</p>

### Pager Connection Options

Enter the information required for the selected Pager Connection option:

GUI Element	Description
<b>Modem number</b>	Enter the phone number to use for sending alphanumeric pages to the paging service modem.
<b>Modem pin number</b>	Enter the last seven digits of the PIN number for your alphanumeric pager. If you use an alphanumeric paging service, you must enter the phone number to use for sending alphanumeric pages to the paging service modem. This number is provided by your paging service. The paging service sometimes refers to this as the TAP/IXO number.

GUI Element	Description
<b>Phone number</b>	<p>Enter the phone number exactly as you would dial it from your telephone, including other numbers you may need, such as a number to get an outside line. You can use dashes to make the number easier to read. Use commas to separate the portions of the phone number. Each comma causes the modem script to pause for a few seconds before dialing the rest of the number.</p> <p><b>Example:</b> If you are dialing your pager from your office, and you have to dial 9 to get an outside line, enter: 9, 555-6789.</p>
<b>Send page command</b>	<p>Enter the page command exactly as you would dial it from your touch tone telephone.</p>
<b>Custom modem command</b>	<p>Enter the entire modem command including the phone number to dial, any additional digits, and \$message. SiteScope replaces \$message with the message you specified for each alert.</p> <p><b>Example:</b> If the number for the pager company is 123-4567, your pager PIN is 333-3333, and your pager company requires that you follow each command with the # key, the command might look like this:  ATDT 123-4567,,333-3333#,, \$message#</p> <p><b>Note:</b> For SiteScope running on UNIX, enter the device path for your modem in the <b>Modem Path</b> box. To see a list of devices using Solaris, use the <code>ls /dev/term/*</code> command.</p>
<b>Disabled</b>	<p>Select to temporarily disable a particular pager without editing every alert that contains this persons pager.</p> <p><b>Default value:</b> Not selected</p>

## Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Schedule</b>	<p>Specifies when pager settings should be enabled. A more restricted schedule can be selected from the drop-down list.</p> <p><b>Default value:</b> every day, all day</p>
<b>Description</b>	<p>Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the &lt;BR&gt;, &lt;HR&gt;, and &lt;B&gt; tags to control display format and style.</p> <p><b>Note:</b> HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> <li>▶ Tags: <b>script</b>, <b>object</b>, <b>param</b>, <b>frame</b>, <b>iframe</b>.</li> <li>▶ Any tag that contains an attribute starting with <b>on</b> is declined. For example, <b>onhover</b>.</li> <li>▶ Any attribute with <b>javascript</b> as its value.</li> </ul>

## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>
<b>Add Tag</b>	<p>Click to add a new keyword tag.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>



## SNMP Trap Preferences

This chapter includes the main concepts and reference information for SiteScope monitor preferences.

### **This chapter includes:**

#### Concepts

- ▶ SNMP Trap Preferences Overview on page 1481

#### Reference

- ▶ SNMP Trap Preferences User Interface on page 1482

### **SNMP Trap Preferences Overview**

You use SNMP Preferences to configure the settings SiteScope needs to communicate with an external SNMP host or management console. These are the default SNMP parameters for use with SNMP Trap alerts.






The SNMP Preferences page displays the defined custom SNMP Trap profiles or templates to send traps to hosts. The SNMP Trap profile can be associated with one or more SNMP Trap alerts by editing the applicable alert definition.


For details on configuring these preferences, see “SNMP Trap Preferences User Interface” on page 1482.

## SNMP Trap Preferences User Interface



<b>Description</b>	Used to define settings that are used by SiteScope SNMP Trap alerts when sending data to management consoles. SiteScope uses the SiteScope SNMP Trap Alert type to integrate with SNMP-based network management systems.  <b>To access:</b> Select <b>Preferences</b> context > <b>SNMP Preferences</b>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit email, pager and SNMP preferences</b> permissions can create or make changes to SNMP Preferences.</li> <li>▶ You cannot delete an SNMP Trap profile if it is referenced by an alert action. You must change the SNMP Trap in the alert before you can delete the SNMP Trap profile.</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SNMP Trap Preferences Overview” on page 1481</li> <li>▶ “New/Edit SNMP Trap Dialog Box” on page 1484</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click the <b>New SNMP Trap</b> button to create a new SNMP Trap profile. For details on the user interface, see “New/Edit SNMP Trap Dialog Box” on page 1484.
	Click the <b>Edit SNMP Trap</b> button to edit the SNMP Trap profile. For details on the user interface, see “New/Edit SNMP Trap Dialog Box” on page 1484.
	Click the <b>Delete SNMP Trap</b> button to delete the selected SNMP Trap profile from SNMP Preferences.
	Click the <b>Test SNMP Trap</b> button to test that you can send a message to the SNMP trap. Enter a message in the Test SNMP Trap dialog box, and click <b>Test</b> .
	Click the <b>Select All</b> button to select all listed SNMP Trap profiles.

GUI Element	Description
	Click the <b>Clear Selection</b> button to clear the selection.
<b>Default Settings</b>	<p>Click the arrow next to <b>Default Settings</b>, and select an option:</p> <ul style="list-style-type: none"> <li>▶ <b>Edit.</b> Opens the SNMP Trap Preferences Default Settings dialog box which enables you to change the default settings displayed in the New SNMP Trap dialog box. For details on the settings, see “New/Edit SNMP Trap Dialog Box” on page 1484.</li> <li>▶ <b>Test.</b> Opens the Test SNMP Trap dialog box which enables you to test that you can send a message to the default SNMP trap. Enter a message in the Test SNMP Trap dialog box, and click <b>Test</b>.</li> </ul>
<b>Name</b>	The text name string assigned to the setting profile when you create a new SNMP trap profile.
<b>Description</b>	A description of the setting profile that was assigned when creating or editing the profile.
<b>Host</b>	The domain name or IP address of the machine that receives all SNMP trap messages.
<b>Port</b>	The SNMP port to which the trap is sent.

 **New/Edit SNMP Trap Dialog Box**

<p><b>Description</b></p>	<p>Enables you to create a new SNMP Trap profile or edit an existing profile.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>SNMP Preferences</b>. In the SNMP Trap Preferences page:</p> <ul style="list-style-type: none"> <li>➤ Click <b>New SNMP Trap</b>  or</li> <li>➤ Select an existing SNMP Trap profile and click <b>Edit SNMP Trap</b> .</li> </ul>
<p><b>Important Information</b></p>	<p>Only an administrator in SiteScope, or a user granted <b>Edit email, pager and SNMP preferences</b> permissions can create or make changes to SNMP Preferences. For details on this topic, see “User Management Preferences Overview” on page 1498.</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ “SNMP Trap Preferences Overview” on page 1481</li> <li>➤ “SNMP Trap Preferences User Interface” on page 1482</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Name</b>	Enter the text name string assigned to the setting profile when creating a new SNMP recipient.
<b>Description</b>	<p>Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the &lt;BR&gt;, &lt;HR&gt;, and &lt;B&gt; tags to control display format and style.</p> <p><b>Note:</b> HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> <li>➤ Tags: <b>script</b>, <b>object</b>, <b>param</b>, <b>frame</b>, <b>iframe</b>.</li> <li>➤ Any tag that contains an attribute starting with <b>on</b> is declined. For example, <code>onhover</code>.</li> <li>➤ Any attribute with <b>javascript</b> as its value.</li> </ul>
<b>Send to host</b>	<p>Enter the domain name or IP address of the machine that receives all SNMP trap messages. This machine must be running an SNMP console to receive the trap message.</p> <p><b>Examples:</b> <code>snmp.mydomain.com</code> or <code>206.168.191.20</code>.</p>
<b>SNMP port</b>	<p>The SNMP port to which the trap is sent.</p> <p><b>Default value:</b> 162</p>
<b>SNMP community</b>	<p>The default SNMP community name used for sending traps. The community string must match the community string used by the SNMP management console.</p> <p><b>Default value:</b> public</p>

GUI Element	Description
<b>SNMP trap ID</b>	<p>The type of trap to send. There are several predefined ID types for common conditions.</p> <ul style="list-style-type: none"> <li>➤ Select a generic SNMP type from the <b>Generic SNMP trap ID</b> drop-down list.</li> <li>➤ To use an enterprise specific SNMP ID type, enter the number of the specific trap type in the <b>Enterprise-Specific SNMP trap ID</b> box.</li> </ul>
<b>SNMP trap version</b>	<p>Select the default SNMP protocol version number to use. SNMP V1 and V2c are currently supported.</p> <p><b>Default value:</b> V1</p>
<b>SNMP object ID</b>	<p>This identifies to the console the object that sent the message.</p> <ul style="list-style-type: none"> <li>➤ Select one of the predefined objects from the <b>Preconfigured SNMP object IDs</b> drop-down list.</li> <li>➤ To use another object ID, enter the other object ID in the <b>Other SNMP object ID</b> box.</li> </ul>

### Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>&lt;Tag name and values&gt;</b>	<p>Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>
<b>Add Tag</b>	<p>Click to add a new keyword tag.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>

# 125

---

## Schedule Preferences

This chapter includes the main concepts and reference information for SiteScope Schedule Preferences.

### **This chapter includes:**

#### Concepts

- ▶ Schedule Preferences Overview on page 1487

#### Reference

- ▶ Schedule Preferences User Interface on page 1490

### **Schedule Preferences Overview**

SiteScope monitors, alerts, and reports are enabled 24 hours a day, 7 days a week, 365 days a year by default. This means that as long as a monitor is enabled, it is run according to the update frequency specified in the individual monitor configuration. For example, if a monitor is configured to run every 30 seconds, SiteScope attempts to run the monitor every 30 seconds throughout the day. If SiteScope detects an error condition, any alert associated with the monitor is triggered as well, regardless of the time of day.

In some situations, it is useful to enable certain SiteScope actions to correspond with a single event or a particular time of day. For example, you may want to use this type of scheduling for monitors, such as the Link Checking monitor, which you want to run only once a day at a time when the server generally has a lighter load. You use Absolute Schedules to do this.

You may also want to disable certain SiteScope actions based on the schedules of the individuals or groups responsible for the servers and systems being monitored. You use Range Schedules to instruct SiteScope to enable or disable monitors according to time periods that you define.

This section includes:

- ▶ “Absolute Schedules” on page 1488
- ▶ “Range Schedules” on page 1489

## Absolute Schedules

Absolute Scheduling lets you set specific times that a monitor is run on a weekly basis. Absolute schedules are reset at the end of the week and repeated each week. Absolute Schedules trigger a monitor to run only once at each time specified in the schedule.

Absolute Schedules are inactive until they are explicitly associated with a monitor instance. To associate Absolute Schedules with a monitor, use the **Monitor schedule** field in the **Monitor Run Settings** panel for the monitor that you want to schedule.

---

**Note:** Absolute Schedules are associated to alerts indirectly by way of the monitors associated with the alert. Any alerts associated with the monitors disabled by Absolute Schedules are effectively unavailable for the period during which those monitors are disabled. However, if an alert is associated with other monitors that are not controlled by the same schedule, that alert is still triggered if the other monitors report an error condition.

---

For details on configuring Absolute Schedule preferences, see “Absolute Schedule Page” on page 1490.



## Range Schedules

You can use Range Scheduling to specify a time range during which SiteScope either enables or disables particular monitors. If you specify an enabled time range for a monitor (in the **Monitor schedule** field of the **Monitor Run Settings** panel for the specific monitor), SiteScope only runs the monitor during that range. For example, if you create a range of 8AM-9PM, Monday through Friday, any monitors that have that range schedule associated with them are run only during those times.

A common use of range scheduling is to set up different pager alerts associated with monitors running at times that coincide with work shifts when different administrators are on call. The schedule helps prevent pager alerts being sent to individuals at an inappropriate time of day relative to the work schedule of that individual.

Range Schedule Preferences are inactive until they are explicitly associated with a monitor instance. You use the Monitor Run Settings panel of a monitor configuration page to associate Range Schedule Preferences with a monitor.

---

**Note:** Range Schedules are associated to alerts indirectly by way of the monitors associated with the alert. Any alerts associated with the monitors disabled by Range Schedules are effectively unavailable for the period during which those monitors are disabled. However, if an alert is associated with other monitors that are not controlled by the same schedule, that alert is still triggered if the other monitors report an error condition.

---


For details on configuring Range Schedule preferences, see “Range Schedule User Page” on page 1492.

## Schedule Preferences User Interface

**This section includes:**

- ▶ Absolute Schedule Page on page 1490
- ▶ Range Schedule User Page on page 1492

## Absolute Schedule Page

<b>Description</b>	<p>Used for customizing the operation of SiteScope monitors and alerts to run only at specific times.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Schedule Preferences</b>. In the Schedule toolbar, click the <b>New</b>  button, and select <b>New Absolute Schedule</b>.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit schedule preferences</b> permissions can create or make changes to Schedule Preferences.</li> <li>▶ You cannot delete an Absolute Schedule profile if it is referenced by an alert action, report, monitor, or monitor threshold. You must remove the profile from each dependency before you can delete the profile.</li> </ul>
<b>Useful Links</b>	<p>“Schedule Preferences Overview” on page 1487</p>

## General Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Name</b>	Enter a name for the Absolute Schedule. The name is used to identify the Absolute Schedule in the product display.
<b>Description</b>	<p>Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the &lt;BR&gt;, &lt;HR&gt;, and &lt;B&gt; tags to control display format and style.</p> <p><b>Note:</b> HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> <li>➤ Tags: <b>script</b>, <b>object</b>, <b>param</b>, <b>frame</b>, <b>iframe</b>.</li> <li>➤ Any tag that contains an attribute starting with <b>on</b> is declined. For example, <b>onhover</b>.</li> <li>➤ Any attribute with <b>javascript</b> as its value.</li> </ul>

## Absolute Schedule Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):


GUI Element	Description
<days of the week>	<p>Enter the time or times that the monitor needs to run in the boxes next to the day of the week. Time values for absolute schedules must be limited to the 24-hour period of a standard day for each day. To enter multiple times for a single day, separate the times by a comma (,).</p> <p><b>Example:</b> 01,02:30,23:30 runs the monitor at 1:00 AM, 2:30 AM, and 11:30 PM</p>

## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>
Add Tag	<p>Click to add a new keyword tag.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>

## Range Schedule User Page

Description	<p>Used for customizing the operation of SiteScope monitors and alerts to run only during specific time periods.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Schedule Preferences</b>. In the Schedule toolbar, click the <b>New</b>  button, and select <b>New Range Schedule</b>.</p>
Important Information	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit schedule preferences</b> permissions can create or make changes to Schedule Preferences.</li> <li>▶ You cannot delete a Range Schedule profile if it is referenced by an alert action, report, monitor, or monitor threshold. You must remove the profile from each dependency before you can delete the profile.</li> </ul>
Useful Links	<p>“Schedule Preferences Overview” on page 1487</p>

## General Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Name</b>	Enter a name for the Range Schedule.
<b>Description</b>	<p>Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the &lt;BR&gt;, &lt;HR&gt;, and &lt;B&gt; tags to control display format and style.</p> <p><b>Note:</b> HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> <li>▶ Tags: <b>script</b>, <b>object</b>, <b>param</b>, <b>frame</b>, <b>iframe</b>.</li> <li>▶ Any tag that contains an attribute starting with <b>on</b> is declined. For example, <b>onhover</b>.</li> <li>▶ Any attribute with <b>javascript</b> as its value.</li> </ul>

## Range Schedule Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<days of the week>	<p>Select the day of the week and enter the time or times the monitor needs to run. Time values for range schedules must be limited to the 24 hour period of a standard day for each day. Select <b>Enabled</b> to run monitors during the specified time range only, or <b>Disabled</b> to run monitors during all hours of the applicable day, except during the time range.</p> <p><b>Note:</b> The range schedule uses a 24 hour time format only.</p> <p><b>Example:</b> To disable monitors from 6:00 PM on Thursday evening until 8:00 AM the following morning, enter a <b>From</b> value of 18 and a <b>To</b> value of 24 for Thursday and then enter a <b>From</b> value of 0 and a <b>To</b> value of 8 for Friday. If you enter a <b>From</b> value of 18 and a <b>To</b> value of 8 on the Thursday schedule, the schedule becomes invalid.</p> <p>To enter multiple times for a single day, separate the times by a comma (.). For example, to disable from 2-3AM and 7-8AM, in the <b>From</b> box enter 2:00,7:00 and in the <b>To</b> box enter 3:00,8:00.</p> <p><b>Default value:</b> Enabled (no time values specified). See the table below for more information.</p>

## Days of the Week

Enable Setting (Enable / Disable)	Time Range (From /To)	Schedule Effect
Enable	<b>From</b> and <b>To</b> time values specified	Monitors are enabled to run only during the <b>From</b> and <b>To</b> time range.
Enable	(no time values specified)	Monitors are enabled to run during all hours of the applicable day. This is the default setting for 24-hour operation.
Disable	<b>From</b> and <b>To</b> time values specified	Monitors are enabled to run during all hours of the applicable day, except during the <b>From</b> and <b>To</b> time range.
Disable	(no time values specified)	Monitors are disabled during all hours of the applicable day.

## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.  For details on using tags, see “Working with Search/Filter Tags” on page 107.
Add Tag	Click to add a new keyword tag.  For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.





# 126

---

## User Management Preferences

This chapter includes the main concepts and reference information for SiteScope User Management Preferences.

**This chapter includes:**

**Concepts**

- ▶ User Management Preferences Overview on page 1498

**Reference**

- ▶ Password Requirement Parameters on page 1503
- ▶ User Management Preferences User Interface on page 1504

## User Management Preferences Overview

---

**Note:** User Management Preferences are available only to users accessing SiteScope directly and not to users accessing SiteScope using System Availability Management Administration in HP Business Availability Center. For details on how SiteScope permissions interact with HP Business Availability Center, see “Accessing SiteScope and Building Permissions Model” on page 163.

---

You manage SiteScope user accounts from the User Management Preferences page. This page enables you to administer the users that are allowed access to SiteScope.

As a client-server based architecture, a single SiteScope user profile can be accessed by multiple users simultaneously. You can define multiple SiteScope user accounts that provide different views and edit permissions for different audiences. For example, you can create a user profile that allows users to view monitor status and reports but does not enable the users to add or edit monitor configurations or alerts.

A user profile limits access to SiteScope to those users that enter a correct user name and password. Optionally, user authentication can be handled by submitting a query to an LDAP database. For more restrictive access control to SiteScope, see “General Preferences User Interface” on page 1379.

A user profile has two main components:

- ▶ User authentication information and access permission
- ▶ Action permissions

Configure these settings for each user profile in the applicable User Profile container.

This section includes:

- ▶ “User Types” on page 1499
- ▶ “User Permissions” on page 1500

- “Notes on User Accounts” on page 1501
- “Changing a User’s Password” on page 1502
- “Configuring User Management Preferences” on page 1502

## User Types

SiteScope provides the following user types:

- **Administrator.** SiteScope provides a single administrator by default. An administrator can view and change anything in SiteScope. It has other special properties as well, such as being allowed to create other users and to change their profiles in the User Management Preferences page. The administrator account cannot be disabled or deleted.
- **Power user (super user).** A power user is a regular user that has been granted user management permissions. A power user can create, edit, or delete other users, except the administrator. A power user can also edit, but not delete, himself. Both an administrator and a power user can create a power user. There may exist any number of power users. For details about enabling this user type, see “Permissions” on page 1509.
- **Regular User.** A regular user cannot create, delete, or edit any user, including itself. It has all the permissions defined for it by the administrator or power user. By default, a regular user is granted all permissions except **Edit user preferences** (under **User Management Preferences**). This limits the user to being able to view their own user properties and the root groups for which they have permissions. A regular user cannot view or edit settings and permissions of other users.

## User Permissions

When setting up SiteScope user accounts, the administrator in SiteScope or a power user can configure the permissions required for different users. Permissions limit the areas in SiteScope that a user can access, and control the types of action a user can perform on SiteScope objects, such as groups, monitors, alerts, reports, preferences, remote servers, templates, and Dashboard.

---

**Note:** By default, a regular user can view their own user properties and the root groups for which they have permissions only. If a regular user is granted **Edit user preferences** permissions (thereby making the user a power user), the user can edit its own settings and permissions, and create and make changes to the settings and permissions of other users.

---

User permissions have been extended in SiteScope so that there are specific view, edit, and test permissions for each preference type, and view, edit, and test permissions for remote servers. This enables the administrator or power user to restrict access for selected users to specific preference types and to remote server properties. Where a user does not have view permissions to a specific preference, the tab for that preference is unavailable.

When selecting permissions for an action type, it is important to understand that there are dependency relationships between certain permissions. Edit and test permissions are always dependent on the corresponding view permission. For example, if you select the **Edit remote servers** or **Test remote servers** permission, the **View remote servers** permission is automatically selected. Conversely, if you clear the **View remote servers** permission, the **Edit remote servers** and **Test remote servers** permissions are automatically cleared.

You configure user permissions from the **Permissions** pane of the New/Edit User dialog box. For details on SiteScope user permissions, see “Permissions” on page 1509.

### Notes and Limitations

- The user preference permissions in SiteScope 10.10 are not supported in System Availability Management Administration when the SiteScope is reporting to HP Business Availability Center version 8.00 or earlier.
- When upgrading from earlier versions of SiteScope to SiteScope 10.10, the new permission values are determined as follows:
  - **View <preference type>** permission is selected by default for all preference types (since there was no corresponding preference permission in earlier versions of SiteScope).
  - **Edit <preference type>** permission for all preference types is determined according to the **Edit Preferences** permission in the earlier version of SiteScope.
  - **Test <preference type>** permission for all preference types is determined according to the **Test Preferences** permission in the earlier version of SiteScope.

### Notes on User Accounts

- The administrator account is the default account used when accessing SiteScope. This means that anyone requesting the server address and port number where SiteScope is running is, by default, logged in on the administrator account. To restrict access to this account and its privileges, you must edit the administrator account profile to include a user login name and login password. SiteScope then displays a login dialog before SiteScope can be accessed.
- You can create a named user account that does not require a user login name and password. You do this by creating a new user profile in the standard format (providing a **Displayed user name**), but leave the **Login name** and **Password** boxes blank. With this configuration, users accessing SiteScope are presented with an authentication dialogue. They may be authenticated as this named user by leaving the **Login Name** and **Password** boxes blank and clicking the **Log In** button. This user is displayed as **guest** on the upper right side of the SiteScope UI.
- You should restrict the permissions on regular user accounts to avoid unauthorized changes to your SiteScope configuration.

## Changing a User's Password

You can change a user's password by clicking the **Change Password** link in the SiteScope Login window, and entering the user's user name, current password, and a new password in the Change Password dialog box.

If the new password does not comply with password configuration rules, an error message is displayed and the password is not changed. For password configuration rules, see "Password Requirement Parameters" on page 1503.

---

**Note:** The SiteScope login password is case sensitive.

---

## Configuring User Management Preferences

For information on configuring User Management Preferences, see "User Management Preferences User Interface" on page 1504.

## Password Requirement Parameters




You can configure password requirements by setting the following parameters in `<SiteScope root directory>\groups\master.config`:

Parameter	Description
<code>_adminMinimumLength = x</code>	The password length must be at least <b>x</b> characters.
<code>_adminRequireAlpha = (1,0)</code>	<ul style="list-style-type: none"> <li>▶ <b>0.</b> Password does not require an alphabetic character.</li> <li>▶ <b>1.</b> Password must contain an alphabetic character.</li> </ul>
<code>_adminRequireNumber = (1,0)</code>	<ul style="list-style-type: none"> <li>▶ <b>0.</b> Password does not require a numeric character.</li> <li>▶ <b>1.</b> Password must contain a numeric character.</li> </ul>
<code>_adminRequirePunctuation = (1,0)</code>	<ul style="list-style-type: none"> <li>▶ <b>0.</b> Password does not require punctuation.</li> <li>▶ <b>1.</b> Password must contain punctuation.</li> </ul>



## User Management Preferences User Interface

<b>Description</b>	<p>The data provided by SiteScope can be made available to multiple users without granting full administrative privileges to all users. This page allows you to create multiple user accounts that provide different view and edit permissions for different audiences.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>User Management Preferences</b></p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit user preferences</b> permissions can create or make changes to user settings and permissions for the current user or for other users. By default, a regular user does not have <b>Edit user preferences</b> permissions, which means that they can view only their own user properties.</li> <li>▶ The Administrator account is the default account that is active when the product is installed. To create other accounts, you must first edit the Administrator account profile to include a user login name and login password.</li> </ul>
<b>Useful Links</b>	<p>“User Management Preferences Overview” on page 1498</p>



The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
	<p>Click the <b>New User</b> button to create a new user profile. For details on the user interface, see “New/Edit User Profile Dialog Box” on page 1505.</p>
	<p>Click the <b>Edit User</b> button to edit the selected user profile. For details on the user interface, see “New/Edit User Profile Dialog Box” on page 1505.</p>
	<p>Click the <b>Delete User</b> button to delete the selected user profiles.</p>



GUI Element	Description
	Click the <b>Select All</b> button to select all listed user profiles.
	Click the <b>Clear Selection</b> button to clear the selection.
<b>Displayed User Name</b>	The title for this user profile that was provided in the <b>Displayed user name</b> box. If a name was not provided, the <b>Login name</b> value is used instead.
<b>Login Name</b>	Displays the login name.
<b>Login Disabled</b>	Displays the login status. If the check box is cleared, access to SiteScope using the user profile is enabled. If the check box is selected, access to SiteScope with this user profile is not allowed.
<b>User Type</b>	The type of user. For details on the different user types, see “User Types” on page 1499.

### **New/Edit User Profile Dialog Box**



<b>Description</b>	<p>Enables you to create a new user profile or edit an existing profile.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>User Management Preferences</b>. In the User Management Preferences page:</p> <ul style="list-style-type: none"> <li>▶ Click the <b>New User</b>  button, or</li> <li>▶ Select an existing User profile and click <b>Edit User</b> .</li> </ul>
<b>Important Information</b>	<p>Only an administrator in SiteScope, or a user granted <b>Edit user preferences</b> permissions can create or make changes to user settings and permissions for the current user or for other users. By default, a regular user does not have <b>Edit user preferences</b> permissions, which means that they can view only their own user properties.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “User Management Preferences Overview” on page 1498</li> <li>▶ “User Management Preferences User Interface” on page 1504</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Displayed user name</b>	(Optional) Enter a title for this User profile. The title is displayed in the list of users. If you do not enter a title, the <b>Login name</b> value is used as the Displayed user name.
<b>Login name</b>	<p>Enter the SiteScope login name to access SiteScope using this profile.</p> <p>Alternatively, users can log into SiteScope using LDAP authentication by entering a value in the relevant LDAP cells.</p> <p><b>Allowed characters:</b> Latin alphanumeric.</p> <p><b>Note:</b> Entering characters other than the allowed characters does not cause an error when creating the user profile. However, the user cannot log in to SiteScope using that login name.</p>
<b>Password</b>	<p>Enter the SiteScope login password for this user.</p> <p>If using LDAP for user authentication, there is no need to enter a password here. Users enter their LDAP password in the SiteScope login dialog box when they log in to their user account.</p> <p>For information about password requirements, see “Changing a User’s Password” on page 1502.</p> <p>All SiteScope passwords are encrypted using 3DES (also known as TDES or Triple Data Encryption Algorithm). Although the TDES key is stored in SiteScope, it cannot be modified. For more information, refer to “Hardening the SiteScope Platform” in the <i>HP SiteScope Deployment Guide</i> PDF.</p> <p><b>Note:</b> The SiteScope login password is case sensitive.</p>
<b>Confirm password</b>	Re-enter the password entered in the <b>Password</b> box. This is used when creating a new user profile or changing the password of an existing user profile.

GUI Element	Description
<b>LDAP service provider</b>	<p>To access the SiteScope service using a centralized LDAP authentication rather than the SiteScope specific password, enter the URL of the applicable LDAP server. This way, password authentication for access to SiteScope can be performed by LDAP.</p> <p><b>Example:</b> ldap://ldap.mydomain.com:389.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▶ Users still need to have a SiteScope login name defined.</li> <li>▶ Users can use LDAP to access SiteScope, but they must have a user login and security principal assigned to them on the LDAP server.</li> </ul>
<b>LDAP security principal</b>	<p>When using LDAP authentication to access the SiteScope service, enter the Security Principal for this user.</p> <p><b>Example:</b> uid=testuser,ou=TEST,o=this-company.com</p> <p><b>Note:</b> Users may be defined with special characters on the LDAP server. However, SiteScope does not support users that contain the following characters in their user name: equal ("="), semi-colon (";"), inverted commas (""). A user name containing invalid characters is unable to log in to SiteScope.</p>
<b>Login disabled</b>	<p>Select to disable access to SiteScope with this user name and password. Clear the check box to enable access using the user profile.</p>

GUI Element	Description
<p><b>Allowed groups</b></p>	<p>Displays the list of groups that can be accessed by this user profile. Click the <b>New</b>  button to open the Select User's Allowed Groups dialog box, and select groups. For details on the user interface, see "Select User's Allowed Groups Dialog Box" on page 1521.</p> <p>To remove user access to a group, select the group and click the <b>Delete</b>  button. It is not possible to delete all groups in the list.</p> <p><b>Default value:</b> The SiteScope node is checked to enable access to all groups.</p> <p><b>Note:</b> This field is not visible for an Administrator's settings.</p>

## Permissions

**Note:** The Permissions pane is not visible for the administrator's account, since they have full permissions which cannot be changed.

<b>Description</b>	Enables you to determine user action permissions. To grant a permission, select the check box to the left of the permission or permission group. A <input checked="" type="checkbox"/> icon displayed to the left of a permission group indicates that not all permissions contained within that root group have been selected.
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit user preferences</b> permissions can create or make changes to user settings and permissions for the current user or for other users.</li> <li>▶ All the permissions in the Permissions pane are selected by default, except for the <b>Edit user preferences</b> permissions which must be granted by the SiteScope administrator.</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “User Management Preferences Overview” on page 1498</li> <li>▶ “User Management Preferences User Interface” on page 1504</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Groups</b>	
<b>Edit groups</b>	Enables the user to add new groups, rename, copy, or delete existing monitor groups. For details, see “New SiteScope Group Dialog Box” on page 297. <b>Default value:</b> Selected
<b>Refresh groups</b>	Enables the user to refresh or force all the monitors within a group to run regardless of their schedule. For details, see “New SiteScope Group Dialog Box” on page 297. <b>Default value:</b> Selected
<b>Disable groups</b>	Enables the user to disable groups. For details, see “Enable/Disable Monitor or Monitors in Group Dialog Box” on page 1879. <b>Default value:</b> Selected
<b>Monitors</b>	
<b>Edit monitors</b>	Enables the user to add new monitors, edit existing monitor configurations, or delete monitors. For details, see “Working with SiteScope Monitors” on page 301. <b>Default value:</b> Selected

GUI Element	Description
<b>Refresh monitors</b>	<p>Enables the user to refresh or force individual monitors to run regardless of their schedule. For details, see “Working with SiteScope Monitors” on page 301.</p> <p><b>Default value:</b> Selected</p>
<b>Acknowledge monitors</b>	<p>Enables the user to use the Acknowledge function to comment on monitor status on the group detail page. For details, see “Acknowledging Monitor Status” on page 1850.</p> <p><b>Default value:</b> Selected</p>
<b>Disable monitors</b>	<p>Enables the user to disable monitors within a group. “Enable/Disable Monitor or Monitors in Group Dialog Box” on page 1879.</p> <p><b>Default value:</b> Selected</p>
<b>Alerts</b>	
<b>View alerts list</b>	<p>Enables the user to view the list of currently configured alert definitions on the Alert List page. This is a root permission that is required to edit, test, or disable alerts indefinitely. For details, see “SiteScope Alerts Page” on page 1997.</p> <p><b>Default value:</b> Selected</p>
<b>Edit alerts</b>	<p>Enables the user to add a new alert, edit, or delete existing alerts. This option is dependent on the <b>View alerts list</b> permission. For details, see “New/Edit Alert Dialog Box” on page 1999.</p> <p><b>Note:</b> Since alert actions are not controlled by alert action preferences permissions, this permission is not dependent on the <b>View emails, pagers, and SNMP lists</b> permission.</p> <p><b>Default value:</b> Selected</p>

GUI Element	Description
<b>Test alerts</b>	Enables the user to test an existing alert definition. This option is dependent on the <b>View alerts list</b> permission. For details, see “SiteScope Alerts Page” on page 1997. <b>Default value:</b> Selected
<b>Disable alerts indefinitely</b>	Enables the user to disable or enable one or more alerts indefinitely. This option is dependent on the <b>View alerts list</b> permission. For details, see “New/Edit Alert Dialog Box” on page 1999. <b>Default value:</b> Selected
<b>Disable alerts temporarily</b>	Enables the user to disable or enable one or more alerts temporarily. For details, see “New/Edit Alert Dialog Box” on page 1999. <b>Default value:</b> Selected
<b>Reports</b>	
<b>Generate monitor summary report</b>	Enables the user to use the Browse Monitor form and the Monitor Summary Report. For details, see “Monitor Summary Report” on page 2080. <b>Default value:</b> Selected
<b>Generate management report</b>	Enables the user to create a scheduled Management report manually. For details, see “Management Report” on page 2072. <b>Default value:</b> Selected
<b>Edit management report</b>	Enables the user to add new report definitions, and edit or delete existing report definitions. For details, see “Management Report” on page 2072. <b>Default value:</b> Selected



GUI Element	Description
<b>Generate quick report</b>	Enables the user to create ad hoc SiteScope management reports. For details, see “Quick Report” on page 2076. <b>Default value:</b> Selected
<b>Generate alert report</b>	Enables the user to create ad hoc or quick alert reports. For details, see “Alert Report” on page 2083. <b>Default value:</b> Selected
<b>Remote Servers</b>	
<b>View remote servers list</b>	Enables the user to view the list of remote servers configured in SiteScope. This is a root permission that is required to edit or test remote servers. For details, see “Remote Server Properties Page” on page 1288.  If this option is not selected, the following entities are not available: <ul style="list-style-type: none"><li>▶ Remote servers tree and remote servers page in the <b>Remote Servers</b> context.</li><li>▶ <b>Add Remote Servers</b> button in the Monitors context.</li></ul> <b>Default value:</b> Selected
<b>Edit remote servers</b>	Enables the user to add remote servers to SiteScope and edit remote server settings. This option is dependent on the <b>View remote servers list</b> permission. For details, see “Remote Server Properties Page” on page 1288. <b>Default value:</b> Selected
<b>Test remote servers</b>	Enables the user to test remote server connectivity. This option is dependent on the <b>View remote servers list</b> permission. For details, see “Remote Server Properties Page” on page 1288. <b>Default value:</b> Selected

GUI Element	Description
<b>General Preferences</b>	
<b>View general preferences</b>	<p>Enables the user to view General Preferences. This is a root permission that is required to edit General Preferences. For details, see “General Preferences User Interface” on page 1379.</p> <p><b>Default value:</b> Selected</p>
<b>Edit general preferences</b>	<p>Enables the user to edit General Preferences. This option is dependent on the <b>View general preferences</b> permission. For details, see “General Preferences User Interface” on page 1379.</p> <p><b>Default value:</b> Selected</p>
<b>Infrastructure Preferences</b>	
<b>View infrastructure preferences</b>	<p>Enables the user to view Infrastructure Preferences. This is a root permission that is required to edit Infrastructure Preferences. For details, see “Infrastructure Preferences User Interface” on page 1388.</p> <p><b>Default value:</b> Selected</p>
<b>Edit infrastructure preferences</b>	<p>Enables the user to edit Infrastructure Preferences. This option is dependent on the <b>View infrastructure preferences</b> permission. For details, see “Infrastructure Preferences User Interface” on page 1388.</p> <p><b>Default value:</b> Selected</p>
<b>Integration Preferences</b>	
<b>View integration preferences</b>	<p>Enables the user to view Integration Preferences. This is a root permission that is required to edit Integration Preferences. For details, see “Integration Preferences User Interface” on page 1429.</p> <p><b>Default value:</b> Selected</p>


GUI Element	Description
<b>Edit integration preferences</b>	<p>Enables the user to create or edit Integration Preferences. This option is dependent on the <b>View integration preferences</b> permission. For details, see “Integration Preferences User Interface” on page 1429.</p> <p><b>Default value:</b> Selected</p>
<b>Failover Preferences</b>	
<b>View failover preferences</b>	<p>Enables the user to view Failover Preferences (see “Failover Preferences” on page 1457). This is a root permission that is required to edit Failover Preferences. For details, see “Failover Preferences User Interface” on page 1458.</p> <p><b>Default value:</b> Selected</p>
<b>Edit failover preferences</b>	<p>Enables the user to edit Failover Preferences. This option is dependent on the <b>View failover preferences</b> permission. For details, see “Failover Preferences User Interface” on page 1458.</p> <p><b>Default value:</b> Selected</p>
<b>Log Preferences</b>	
<b>View log preferences</b>	<p>Enables the user to view Log Preferences. This is a root permission that is required to edit Log Preferences. For details, see “Log Preferences User Interface” on page 1452</p> <p><b>Default value:</b> Selected</p>
<b>Edit log preferences</b>	<p>Enables the user to edit Log Preferences. This option is dependent on the <b>View log preferences</b> permission. For details, see “Log Preferences User Interface” on page 1452</p> <p><b>Default value:</b> Selected</p>

GUI Element	Description
<b>Email, Pager, and SNMP Preferences</b>	
<b>View email, pager and SNMP lists</b>	<p>Enables the user to view the Email, Pager, and SNMP profile lists. This is a root permission that is required to edit or test Email, Pager, and SNMP Preferences.</p> <p>For details, see “Email Preferences User Interface” on page 1462, “Pager Preferences User Interface” on page 1473, and “SNMP Trap Preferences User Interface” on page 1482.</p> <p><b>Default value:</b> Selected</p>
<b>Edit email, pager and SNMP preferences</b>	<p>Enables the user to create or edit Email, Pager, and SNMP Preferences. This option is dependent on the <b>View email, pager and SNMP lists</b> permission.</p> <p>For details, see “Email Preferences User Interface” on page 1462, “Pager Preferences User Interface” on page 1473, and “SNMP Trap Preferences User Interface” on page 1482.</p> <p><b>Default value:</b> Selected</p>
<b>Test email, pager and SNMP preferences</b>	<p>Enables the user to test any preference setting for communicating with an external service such as email, pager, or SNMP. This option is dependent on the <b>View email, pager and SNMP lists</b> permission.</p> <p>For details, see “Email Preferences User Interface” on page 1462, “Pager Preferences User Interface” on page 1473, and “SNMP Trap Preferences User Interface” on page 1482.</p> <p><b>Default value:</b> Selected</p>
<b>Schedule Preferences</b>	
<b>View schedule list</b>	<p>Enables the user to view Schedule Preferences. This is a root permission that is required to edit Schedule Preferences. For details, see “Schedule Preferences User Interface” on page 1490.</p> <p><b>Default value:</b> Selected</p>

GUI Element	Description
<b>Edit schedule preferences</b>	<p>Enables the user to create or edit Schedule Preferences. This option is dependent on the <b>View schedule list</b> permission. For details, see “Schedule Preferences User Interface” on page 1490.</p> <p><b>Default value:</b> Selected</p>
<b>User Management Preferences</b>	
<b>Edit user preferences</b>	<p>Enables the user to view, edit, or delete user preferences for all other users, except the SiteScope administrator user. A power user cannot delete his/her own account. For users who do not have this permission, the New/Edit User dialog box is displayed as read only, and the settings and root groups for which the current user has permissions are displayed.</p> <p><b>Default value:</b> Not selected</p>
<b>Credential Preferences</b>	
<b>View credential list</b>	<p>Enables the user to view Credential Preferences. This is a root permission that is required to edit Credential Preferences. For details, see “Credential Preferences User Interface” on page 1528.</p> <p>If this option is not selected, the following entities are not available:</p> <ul style="list-style-type: none"> <li>▶ <b>Credential Preferences</b> tab in the Preferences context.</li> <li>▶ <b>Add Credentials</b> button in the Remote Servers and Monitors context.</li> </ul> <p><b>Default value:</b> Selected</p>
<b>Edit credential preferences</b>	<p>Enables the user to create or edit Credential Preferences. This option is dependent on the <b>View credential list</b> permission. For details, see “Credential Preferences User Interface” on page 1528.</p> <p><b>Default value:</b> Selected</p>




GUI Element	Description
<b>Certificate Management</b>	
<b>View certificates list</b>	<p>Enables the user to view the Certificate Management page. This is a root permission that is required to edit Certificate Management. For details, see “Certificate Management User Interface” on page 1538.</p> <p><b>Default value:</b> Selected</p>
<b>Edit certificates list</b>	<p>Enables the user to manage certificates using Certificate Management. This option is dependent on the <b>View certificates list</b> permission. For details, see “Certificate Management User Interface” on page 1538.</p> <p><b>Default value:</b> Selected</p>
<b>Tags</b>	
<b>View tags</b>	<p>Enables the user to view the New/ Edit SiteScope Tag dialog box to see a list of defined tags. This is a root permission that is required to edit tags. For details, see “Search/Filter Tags User Interface” on page 1534.</p> <p><b>Default value:</b> Selected</p>
<b>Edit tags</b>	<p>Enables the user to add, edit, or delete search/filter tags and tag values. This option is dependent on the <b>View tags</b> permission. For details, see “Search/Filter Tags User Interface” on page 1534.</p> <p><b>Default value:</b> Selected</p>
<b>Templates</b>	
<b>View templates</b>	<p>Enables the user to view templates that exist in the monitor tree. This is a root permission that is required to edit templates. For details, see “Template Tree” on page 84.</p> <p><b>Default value:</b> Selected</p>
<b>Edit templates</b>	<p>Enables the user to add, edit, and delete templates. This option is dependent on the <b>View templates</b> permission. For details, see “Template Tree” on page 84.</p> <p><b>Default value:</b> Selected</p>

GUI Element	Description
<b>Dashboard</b>	
<b>Edit favorites</b>	<p>Enables the user to add or delete items in the favorite views list in the Dashboard view. For details, see “Save to Dashboard Favorites Dialog Box” on page 1869 and “Delete Dashboard Favorites Dialog Box” on page 1870.</p> <p><b>Default value:</b> Selected</p>
<b>View monitor history</b>	<p>Enables the user to view the recent history report for a monitor. For details, see “SiteScope Dashboard - Monitor History View” on page 1866.</p> <p><b>Default value:</b> Selected</p>
<b>Other</b>	
<b>Use tools</b>	<p>Enables the user to use SiteScope tools in the Tools container to troubleshoot and diagnose monitor configuration problems. For details, see “SiteScope Tools” on page 193.</p> <p><b>Default value:</b> Selected</p>






GUI Element	Description
<b>View logs</b>	<p>Enables the user to view the raw data reported by SiteScope monitors sent by alerts, and other SiteScope logs. For details, see “Using Log Files” on page 1927.</p> <p><b>Default value:</b> Selected</p>
<b>View server statistics</b>	<p>Enables the user to view SiteScope internal data that can be used for analyzing SiteScope server performance, stability, health, and for debugging bottlenecks. For details, see “Using Server Statistics” on page 1922.</p> <p><b>Default value:</b> Selected</p>
<b>Use monitor tools</b>	<p>Enables the user to use SiteScope tools when configuring or editing particular monitor types. If a diagnostic tool is available for a monitor type, the <b>Tools</b> button  is enabled in the Dashboard toolbar for that monitor in the group detail page. For details, see “SiteScope Tools” on page 193.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ Diagnostic tools may expose sensitive system information.</li> <li>➤ This option is dependent on the <b>Use tools</b> permission.</li> </ul> <p><b>Default value:</b> Selected</p>



## Select User's Allowed Groups Dialog Box

<p><b>Description</b></p>	<p>Enables you to select the groups and/or subgroups that the user is allowed to access.</p> <p>Select the box next to individual groups or subgroups to enable access to that group. By default, access is allowed to all groups. To restrict user access to fewer groups, clear the check box for the SiteScope node and then select the individual groups below the SiteScope node to which you want to enable access.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>User Management Preferences</b>. In the User Management Preferences page, click the <b>New User</b>  button, or select an existing user profile and click <b>Edit User</b> . In the New/Edit User dialog box, click the <b>New</b>  button in the <b>Allowed groups</b> area.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>➤ Only an administrator in SiteScope, or a user granted <b>Edit user preferences</b> permissions can create or make changes to user settings and permissions for the current user or for other users. By default, a regular user does not have <b>Edit user preferences</b> permissions, which means that they can view only their own user properties.</li> <li>➤ When selected, each of a group's subgroups are also added to the list of allowed groups.</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ "User Management Preferences Overview" on page 1498</li> <li>➤ "User Management Preferences User Interface" on page 1504</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
 SiteScope	Represents an individual SiteScope server. <b>Default value:</b> The current container and all child elements are selected.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors). If an alert has been set up for the monitor group or subgroup, the alert  symbol is displayed next to the group icon. If a Management report has been set up for the monitor group or subgroup, the report  symbol is displayed next to the group icon.
	Represents the collection of available health monitors that are deployed to check proper functioning of SiteScope monitors.

# 127

---

## Credential Preferences

This chapter includes the main concepts, tasks, and reference information for SiteScope Credential Preferences.

**This chapter includes:**

**Concepts**

- ▶ Credential Preferences Overview on page 1524

**Tasks**

- ▶ Configure Credential Preferences on page 1527

**Reference**

- ▶ Credential Preferences User Interface on page 1528

## Credential Preferences Overview

Credential Preferences provide centralized credential management for SiteScope resources. It enables you to input user names and passwords for SiteScope monitors, templates, and remote hosts once as a credential profile, and then have SiteScope automatically supply that information when you configure those resources.

Using Credential Preferences enables you to:

- ▶ Create and manage your credentials. You can add, modify, and delete credentials from one central location.
- ▶ Update credentials. If credentials for a resource expire or need to be updated, the credential profile can be updated and the changes are applied to all usages of the resource within SiteScope. This saves having to find and manually update all usages of the resource in SiteScope.
- ▶ Keep user credentials secure. All passwords stored in Credential Preferences are encrypted. Only an administrator, or a user granted **Edit credential preferences** permissions, can make changes to the credentials.
- ▶ Search and replace by credential properties, and replace credentials with other credentials using Global Search and Replace.
- ▶ Copy monitors in SiteScope with their credential settings. You can also copy monitors to other SiteScopes when there is more than one SiteScope connected to Business Availability Center (only available through System Availability Management Administration). If a credential profile does not exist in the SiteScope to which the monitor is copied, the credential profile is created in that SiteScope.

This section includes:

- ▶ “Monitoring Credential Profiles” on page 1525
- ▶ “Supported Monitors” on page 1525
- ▶ “Notes” on page 1526
- ▶ “Configuring Credential Preferences” on page 1526

## Monitoring Credential Profiles

If user credentials expire or change, the monitors using these credentials fail and are in **Error** status. To avoid this situation, you can create a monitor for each credential profile that checks the authentication, and makes all monitors of the monitor type dependent on the test monitor.

For example, you can create an IPMI monitor, `IPMI_test_credentials`, and manually configure the server login and password. When you configure your IPMI monitors, in the Dependencies panel, enter `IPMI_test_credentials` in the **Depends on** box and select Available as the **Depends condition**. If the `IPMI_test_credentials` monitor becomes unavailable for any reason, the IPMI monitors are automatically disabled.

## Supported Monitors

You can use Credential Preferences to store credentials for the following monitors:

Monitor Category	Monitor
Application	<ul style="list-style-type: none"> <li>➤ COM+ Server</li> <li>➤ SAP CCMS</li> <li>➤ SAP CCMS Alert</li> <li>➤ SAP Java Web Application Server</li> <li>➤ SAP Performance</li> <li>➤ SAP Work Processes</li> <li>➤ Siebel Application Server</li> <li>➤ WebSphere Application Server</li> </ul>
Database	<ul style="list-style-type: none"> <li>➤ Database Counter</li> <li>➤ DB2 8.x</li> <li>➤ Oracle Database</li> </ul>
Server	<ul style="list-style-type: none"> <li>➤ IPMI</li> </ul>
Web Transaction	<ul style="list-style-type: none"> <li>➤ URL</li> <li>➤ URL Content</li> <li>➤ URL List</li> </ul>

## Notes

- ▶ Copying credential settings to other SiteScopes is not supported when copying monitors to older versions of SiteScope.
- ▶ You cannot delete a credential profile if it is referenced by a monitor or a remote host. You must remove the credential profile from each dependency before you can delete the credential profile.
- ▶ If a credential that is used in a template remote host or template monitor has been deleted, you must add the missing credential to Credential Preferences or manually enter credentials for the resource in the template object before deploying the template.

## Configuring Credential Preferences

For task details, see “Configure Credential Preferences” on page 1527.

For user interface details, see “Credential Preferences User Interface” on page 1528.

## Configure Credential Preferences

This task describes the steps involved in configuring and managing credentials for SiteScope objects that require user authentication.

This task includes the following steps:

- “Prerequisites” on page 1527
- “Create a Credential Profile” on page 1527
- “Configure SiteScope Resources Using Credential Profiles” on page 1527
- “Update Credential Profiles” on page 1528
- “Results” on page 1528

### 1 Prerequisites

To create or make changes to the credentials, you must be an administrator in SiteScope, or a user granted **Edit credential preferences** permissions.

For details on user permissions, see “Permissions” on page 1509.

### 2 Create a Credential Profile

Configure a credential profile in Credential Preferences for each SiteScope resource that requires user authentication. For details on the user interface, see “Credential Preferences User Interface” on page 1528.

For a list of supported monitors, see “Supported Monitors” on page 1525.

### 3 Configure SiteScope Resources Using Credential Profiles

When you configure a SiteScope resource that has a credential profile, select the profile in the **Credentials** box in the resource’s settings area.

- For details on the user interface when configuring a monitor, see the Monitor Settings for the specific monitor.
- For details on the user interface when configuring a remote server, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291, and “New/Edit UNIX Remote Servers Dialog Box” on page 1299.

## 4 Update Credential Profiles

If credentials for a resource change, you can update the credential profile without having to find all usages of the resource and update each resource separately in SiteScope. To change a profile, select the profile in Credential Preferences, click **Edit Credential Profile**, and make the necessary changes. For details on the user interface, see “Credential Preferences User Interface” on page 1528.

## 5 Results






SiteScope authenticates the login and password for the resource using the credentials supplied in Credential Preferences.

## Credential Preferences User Interface



<b>Description</b>	Provides centralized credential management for SiteScope resources. This enables you to add, update, and delete credentials that are used in configuring SiteScope monitors, templates, and remote hosts.  <b>To access:</b> Select <b>Preferences</b> context > <b>Credential Preferences</b>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit credential preferences</b> permissions, can create or make changes to Credential Preferences.</li> <li>▶ You cannot delete a credential profile if it is referenced by a monitor. You must remove the profile from each dependency before you can delete the profile.</li> </ul>
<b>Included in Tasks</b>	“Configure Credential Preferences” on page 1527
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Credential Preferences Overview” on page 1524</li> <li>▶ “New/Edit Credential Profile Dialog Box” on page 1530</li> </ul>



The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click the <b>New Credential Profile</b> button to open the New Credential Profile dialog box that enables you to create a new credential profile. For details on the user interface, see “New/Edit Credential Profile Dialog Box” on page 1530.
	Click the <b>Edit Credential Profile</b> button to open the Edit Credential Profile dialog box that enables you to edit a credential profile. For details on the user interface, see “New/Edit Credential Profile Dialog Box” on page 1530.
	Click the <b>Delete Credential Profile</b> button to delete the selected credential profile from Credentials Preferences.
	Click the <b>Select All</b> button to select all listed credential profiles.
	Click the <b>Clear Selection</b> button to clear the selection.
<b>Name</b>	The text name string assigned to the setting profile when you create a new credential profile.
<b>Login</b>	The user name to access the resource using this credential profile.
<b>Description</b>	A description of the setting profile that was assigned when creating or editing the credential profile.

## **New/Edit Credential Profile Dialog Box**

<b>Description</b>	<p>Enables you to create a new credential profile or edit an existing profile. You use credential profiles for storing and managing authentication credentials for SiteScope resources.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Credential Preferences</b>. In the Credentials page:</p> <ul style="list-style-type: none"> <li>▶ Click <b>New</b>  and select <b>New Credentials</b>, or</li> <li>▶ Select an existing credential profile and click <b>Edit</b> .</li> </ul>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user granted <b>Edit credential preferences</b> permissions can create or make changes to Credential Preferences.</li> <li>▶ This page opens in view mode or edit mode depending on your user permissions. For details on this topic, see “User Management Preferences Overview” on page 1498.</li> </ul>
<b>Included in Tasks</b>	“Configure Credential Preferences” on page 1527
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Credential Preferences Overview” on page 1524</li> <li>▶ “Credential Preferences User Interface” on page 1528</li> </ul>

### **Main Settings**

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Name</b>	Enter a descriptive name for the credential profile. <b>Maximum length:</b> 50 characters
<b>Domain</b>	(Optional) Enter the domain for the credential. During the connection, the domain is added to the login in the format: <domain>\<login>.
<b>Login</b>	Enter the user name to access the resource using this credential profile.

GUI Element	Description
<b>Password</b>	<p>Enter the password to access the resource using this credential profile.</p> <p>All SiteScope passwords are encrypted using 3DES (also known as TDES or Triple Data Encryption Algorithm). For more information, refer to “Hardening the SiteScope Platform” in the <i>HP SiteScope Deployment Guide</i> PDF.</p>
<b>Confirm password</b>	<p>Re-enter the password entered in the <b>Password</b> box. This is used when creating a new credential or changing the password of an existing credential.</p>

### Advanced Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Description</b>	<p>Enter a description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the &lt;BR&gt;, &lt;HR&gt;, and &lt;B&gt; tags to control display format and style.</p> <p><b>Note:</b> HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:</p> <ul style="list-style-type: none"> <li>▶ Tags: <b>script</b>, <b>object</b>, <b>param</b>, <b>frame</b>, <b>iframe</b>.</li> <li>▶ Any tag that contains an attribute starting with <b>on</b> is declined. For example, <b>onhover</b>.</li> <li>▶ Any attribute with <b>javascript</b> as its value.</li> </ul>

## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>
<b>Add Tag</b>	<p>Click to add a new keyword tag.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>

## Search/Filter Tags

This chapter includes the main concepts and reference information for SiteScope Search/Filter Tags.

### **This chapter includes:**

#### Concepts

- ▶ Search/Filter Tags Overview on page 1533

#### Reference

- ▶ Search/Filter Tags User Interface on page 1534

### **Search/Filter Tags Overview**

You use Search/Filter Tag Preferences to manage the Search/Filter Tags defined in SiteScope. These tags can be assigned to items in the context tree or preference profiles, and they are used as objects for a filter.






The Search/Filter Tag Preferences page displays the list of Search/Filter Tags. You can add, edit, or delete Search/Filter Tags from this page.

For details on configuring these preferences, see “Search/Filter Tags User Interface” on page 1534.

## Search/Filter Tags User Interface

<b>Description</b>	Used to manage the Search/Filter tags defined in SiteScope. You can assign tags to one or more items in the context trees and preference profiles, and then use the tags as an object for a filter.  <b>To access:</b> Select <b>Preferences</b> context > <b>Search/Filter Tags</b>
<b>Included in Tasks</b>	“Create and Define a New Search/Filter Tag” on page 108
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Working with Search/Filter Tags” on page 107</li> <li>▶ “Search/Filter Tags Overview” on page 1533</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click the <b>New Tag</b> button to open the New Tag dialog box which enables you to create a new search/filter tag. For details on the user interface, see “New/Edit Tag Dialog Box” on page 116.
	Click the <b>Edit Tag</b> button to open the Edit Tag dialog box which enables you to edit a search/filter tag. For details on the user interface, see “New/Edit Tag Dialog Box” on page 116.
	Click the <b>Delete Tags</b> button to delete the selected tag from Search/Filter Tag Preferences.
	Click the <b>Select All</b> button to select all listed search/filter tags.
	Click the <b>Clear Selection</b> button to clear the selection.
<b>Name</b>	The text name string assigned to the setting profile when you create a new search/filter tag.
<b>Description</b>	A description of the setting profile that was assigned when creating or editing the search/filter tag.

# 129

---

## Certificate Management

This chapter includes the main concepts, tasks, and reference information for SiteScope Certificate Management.

**This chapter includes:**

**Concepts**

- ▶ Certificate Management Overview on page 1536

**Tasks**

- ▶ Import Server Certificates Using Certificate Management on page 1537

**Reference**

- ▶ Certificate Management User Interface on page 1538

## Certificate Management Overview

When monitoring a remote server, if the target server uses a self-signed certificate, the certificate must be added to a trusted keystore. If you are monitoring a URL, a WebSphere Application Server, or a VMware-based server using a secure connection, you can manage self-signed certificates from the Certificate Management page.

Benefits of using Certificate Management include:

- ▶ Certificates do not need to be managed using the standard JVM tools (keytool). This avoids the requirement for a desktop/shell session to the SiteScope machine.
- ▶ Provides visual keystore management (add and remove certificates) and enables dynamic keystore reload, without having to restart SiteScope after each certificate change operation.

---

### Note:

- ▶ Only an administrator in SiteScope, or a user with **View/Edit certificates list** permissions can view, add, or make changes to the certificates keystore on the Certificate Management page.
- ▶ Monitors are bound to the keystores that they are using. For URL, WebSphere Application Server, and VMware Performance monitors, the following keystore is used: **<SiteScope root directory>\java\lib\security\cacerts**. Other keystores are ignored.
- ▶ You can still import certificates using the keytool method if preferred. For details on manually importing certificates, see the documentation for the specific monitor type.
- ▶ If you use a self-generated Certificate Authority (CA) certificate to sign all the server certificates, you only need to import the CA certificate once.

---

For details on importing certificates using Certificate Management, see “Import Server Certificates Using Certificate Management” on page 1537.



For details on the user interface, see “Certificate Management Page” on page 1538.

## Import Server Certificates Using Certificate Management

This task describes the steps involved in importing self-signed certificates using Certificate Management.

This task includes the following steps:

- “Prerequisites” on page 1537
- “Import the Server Certificate” on page 1537
- “Configure the Monitor Properties” on page 1538

### 1 Prerequisites

- You can use Certificate Management to import server certificates that are required when configuring secure connections for URL, URL Content, URL List, URL Sequence, VMware Performance, or WebSphere Application Server monitors.
- Only an administrator in SiteScope, or a user with **View/Edit certificates list** permissions can view, add, or make changes to the certificates keystore on the Certificate Management page.

### 2 Import the Server Certificate

If the Web server on which you are monitoring has an `https://` prefix, it is a secure, encrypted connection, and you need to import the server certificate.

- a** Select **Preferences > Certificate Management**, and click the **Import Certificates** button. Select **File** or **Host**, and enter the details of the source server. For details on the Import Certificates dialog box, see “Import Certificates Dialog Box” on page 1540.

- b** From the Loaded Certificates table, select the server certificates to import and click **Import**. The imported certificates are added to the Certificate Management keystore list. For details on the Certificate Management page, see “Certificate Management Page” on page 1538.

### 3 Configure the Monitor Properties

After importing the required server certificates, you can create a monitor with a secured connection.

## Certificate Management User Interface

**This section includes:**






- Certificate Management Page on page 1538
- Import Certificates Dialog Box on page 1540
- Certificate Details Dialog Box on page 1542

## Certificate Management Page

<p><b>Description</b></p>	<p>Used for managing certificates used with SiteScope URL, URL Content, URL List, URL Sequence, VMware Performance, or WebSphere Application Server monitors. The Certificate Management page enables you to add, remove, and refresh keystore contents.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Certificate Management</b>.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>➤ Only an administrator in SiteScope, or a user with <b>View/Edit certificates list</b> permissions can view, add, or make changes to the certificates keystore on the Certificate Management page.</li> <li>➤ You can change the sort order in the columns by clicking the arrow in the column title. A small down or up arrow is displayed indicating the column is sorted in ascending or descending order.</li> </ul>

<b>Included in Tasks</b>	“Import Server Certificates Using Certificate Management” on page 1537
<b>Useful Links</b>	“Certificate Management Overview” on page 1536

The following elements are included (unlabeled GUI elements are shown in angle brackets>):



GUI Element	Description
	Click the <b>Import Certificates</b> button to open the Import Certificates dialog box and add certificates to the Certificate Management keystore list. For details on the user interface, see “Import Certificates Dialog Box” on page 1540.
	Click the <b>Remove Certificates</b> button to delete the selected certificates from the Certificate Management keystore list.
	Click the <b>Reload Certificate List</b> button to reload the keystore certificates from the <b>&lt;SiteScope root directory&gt;\java\lib\security\cacerts</b> files on the remote server. This enables you to manually reload keystore changes without having to restart SiteScope.
	Click the <b>Select All</b> button to select all listed certificates.
	Click the <b>Clear Selection</b> button to clear the selection.
<b>&lt;certificates&gt;</b>	Lists the server certificates that have been imported. Double-click a certificate to open the Certificate Details dialog box and display the certificate’s properties and values. For details on the user interface, see “Certificate Details Dialog Box” on page 1542.
<b>Alias</b>	The certificate alias name. <b>Note:</b> Alias names of imported certificates cannot be modified (they can be modified only during the import certificate step).
<b>Issuer</b>	The name of the certificate issuer.

GUI Element	Description
Valid Until	The time and date until which the certificate is valid.
Version	The certificate version number.

## Import Certificates Dialog Box

<b>Description</b>	<p>Used for adding certificates used with SiteScope URL, WebSphere Application, and VMware Performance monitors to the Certificate Management list keystore. The Certificate Management page enables you to add, remove, and refresh keystore contents.</p> <p><b>To access:</b> Select <b>Preferences</b> context &gt; <b>Certificate Management</b>.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Only an administrator in SiteScope, or a user with <b>View/Edit certificates list</b> permissions can view, add, or make changes to the certificates keystore on the Certificate Management page.</li> <li>▶ You can change the sort order in the columns by clicking the arrow in the column title. A small down or up arrow is displayed indicating the column is sorted in ascending or descending order.</li> </ul>
<b>Included in Tasks</b>	“Import Server Certificates Using Certificate Management” on page 1537
<b>Useful Links</b>	“Certificate Management Overview” on page 1536

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Source Selection</b>	
<b>File</b>	Select this option to add certificates from a file. Click the <b>Select</b> button, navigate to the file from which you want to import certificates, and click <b>Open</b> . Add the required certificates to the Certificate Management list.
<b>Host</b>	Select this option to add certificates from a host server. Enter the real IP address or host name of the monitored server.
<b>Port</b>	Enter the port number of the host machine (available only if the <b>Host</b> option is selected). <b>Default Port value:</b> 443
<b>Load</b>	Click to load certificates for the machine specified in the <b>Host</b> field. The certificates are displayed in the Loaded Certificates table.
<b>Loaded Certificates</b>	
	Click the <b>Select All</b> button to select all listed certificates.
	Click the <b>Clear Selection</b> button to clear the selection.
<b>Alias</b>	The certificate alias name. You can modify a certificate alias during the import certificate step by entering a new alias in the <b>Alias</b> column. <b>Note:</b> An alias name cannot be modified after the certificate has been imported .
<b>Issuer</b>	The name of the certificate issuer.
<b>Valid Until</b>	The time and date until which the certificate is valid.

GUI Element	Description
<b>Version</b>	The certificate version number.
<b>Import</b>	Select the certificates to import from the Loaded Certificates table, and click <b>Import</b> . The imported certificates are displayed in the Certificate Management page.

## Certificate Details Dialog Box

<b>Description</b>	Displays properties and values for the selected server certificate. <b>To access:</b> Select <b>Preferences</b> context > <b>Certificate Management</b> . Double-click a certificate in the Certificate Management page.
<b>Important Information</b>	Only an administrator in SiteScope, or a user with <b>View/Edit certificates list</b> permissions can view, add, or make changes to the certificates keystore on the Certificate Management page.
<b>Useful Links</b>	“Certificate Management Overview” on page 1536

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Alias</b>	The certificate alias name.
<b>Certificate Properties</b>	
<b>Fingerprint</b>	The certificate's fingerprint.
<b>Type</b>	The certificate type.
<b>Version</b>	The certificate version number.
<b>Issuer principal</b>	The name of the certificate issuer.
<b>Serial number</b>	The serial number of the certificate.

GUI Element	Description
<b>Signature algorithm name</b>	The name of the signature algorithm of the certificate.
<b>Valid from</b>	The time and date from which the certificate is valid.
<b>Valid until</b>	The time and date until which the certificate is valid.





# 130

---

## Using SiteScope in an Internationalization (I18N) Environment

This chapter includes the main concepts, tasks, and reference information for working with SiteScope in an I18N environment.

### **This chapter includes:**

#### Concepts

- ▶ Multi-Lingual User (MLU) Interface Support on page 1546

#### Tasks

- ▶ Configure SiteScope for a Non-English Locale on page 1547
- ▶ View SiteScope User Interface in a Specific Language on page 1549

#### Reference

- ▶ Monitors Tested for Internationalization on page 1550

**Troubleshooting and Limitations** on page 1552

## Multi-Lingual User (MLU) Interface Support

The SiteScope user interface can be viewed in the following languages in your Web browser:

Language	Language Preference in Web Browser
English	English
Simplified Chinese	Chinese (China) [zh-cn], Chinese (Singapore) [zh-sg]
Korean	Korean [ko]
Japanese	Japanese [ja]

Use the language preference option in your browser to select how to view SiteScope. The language preference chosen affects only the user's local machine and not the SiteScope machine or any other user accessing the same SiteScope. For details on setting the user interface viewing language, see "View SiteScope User Interface in a Specific Language" on page 1549.

---

**Note:** The language is determined when you log in to SiteScope; changing the language preference in your browser once you have logged in has no affect until you log out and log back in.

---

## Notes and Limitations

- ▶ There is no language pack installation. All translated languages are integrated into SiteScope Multi-lingual User interface (MLU).
- ▶ Data stays in the language it was entered in, even if the language of the Web browser changes. Changing the language of the Web browser on your local machine does not change the language of monitor definitions and configurations.
- ▶ Names of entities included with the SiteScope installation, such as template examples, solution templates, views, and health monitors, are in English only.
- ▶ SiteScope Help can be viewed in Japanese if that is the language that you have selected for the user interface. When you select **Help on this page** or **SiteScope Help**, it is displayed in Japanese. To activate this function, you must install a software patch. Contact HP Software Support (<http://www.hp.com/go/hpsoftwaresupport>) for further information.
- ▶ Other links in the Help drop-down list, such as **Troubleshooting & Knowledge Base**, **HP Software Support**, and **HP Software Web Site**, are also displayed in the user interface language you selected.

## Configure SiteScope for a Non-English Locale

This task describes the steps involved in configuring SiteScope for a non-English locale.

This task includes the following steps:

- ▶ “Change the Locale Version Setting” on page 1548
- ▶ “Set New Locale Time and Data Settings” on page 1548
- ▶ “View SiteScope User Interface in a Specific Language” on page 1548
- ▶ “Results” on page 1548

## 1 Change the Locale Version Setting

In the monitor tree, select **Preferences > General Preferences**. In the Main Panel, select **International version**, and click **Save**. Restart SiteScope. This enables SiteScope to work with multiple character sets.

For details on the user interface, see “International version” on page 1381.

## 2 Set New Locale Time and Data Settings

You can set a new locale time and data settings for SiteScope.

- a** Open `<SiteScope root directory>\groups\master.config` in a text editor.
- b** Find the entry `_localeCountry=`, and assign it an uppercase 2-character ISO-3166 country code. For example: `_localeCountry=US`. A list of country codes is available at [http://www.chemie.fu-berlin.de/diverse/doc/ISO\\_3166.html](http://www.chemie.fu-berlin.de/diverse/doc/ISO_3166.html).
- c** Find the entry `_localeLanguage=`, and assign it a lowercase 2-character ISO-639 language code. For example: `_localeLanguage=en`. A list of language codes is available at <http://www.ics.uci.edu/pub/ietf/http/related/iso639.txt>.
- d** Save the file and restart SiteScope.

## 3 View SiteScope User Interface in a Specific Language

Select a language preference for viewing the SiteScope user interface.

For details on how to perform this task, see “View SiteScope User Interface in a Specific Language” on page 1549.

## 4 Results

SiteScope is configured to work with multiple foreign character sets, the time and data settings are displayed in a locale-specific format, and the user interface is displayed in a foreign language.

## View SiteScope User Interface in a Specific Language

This task describes how to select a language preference for viewing the SiteScope user interface.

---

**Note:** For a list of supported languages, see “Multi-Lingual User (MLU) Interface Support” on page 1546.

---

### To view SiteScope user interface in a specific language:

- 1** Install the required language’s fonts on your local machine if they have not yet been installed. If you choose a language in your Web browser whose fonts have not been installed, the SiteScope user interface uses the default language of your local machine.

For example, the default language on your local machine is English and the Web browser is configured to use Japanese. If Japanese fonts are not installed on the local machine, the SiteScope user interface is displayed in English.

- 2** If you use Internet Explorer, configure the Web browser on your local machine to select the language in which you want to view the SiteScope user interface. For details, see <http://support.microsoft.com/kb/306872/en-us>. Go to step 4.
- 3** If you use FireFox, configure the Web browser on your local machine as follows:
  - a** Select **Tools > Options > Advanced**. Click **Edit Languages**. The Language dialog box opens.
  - b** Highlight the language in which you want to view SiteScope.  
If the language you want is not listed in the dialog box, expand the **Select language to add...** list, select the language, and click **Add**.
  - c** Click **Move Up** to move the selected language to the first row.
  - d** Click **OK** to save the settings. Click **OK** to close the Language dialog box.
- 4** Click **LOGOUT** at the top of the SiteScope window. SiteScope refreshes and the user interface is displayed in the selected language.

## **Monitors Tested for Internationalization**

The following monitors have been tested for internationalization.

### **Monitors Tested for Windows Operating Systems**

- CPU Monitor
- Database Counter Monitor
- Database Query Monitor'
- Disk Space Monitor
- Link Check Transaction Monitor
- Log File Monitor
- Microsoft IIS Server Monitor
- Microsoft SQL Server Monitor
- Microsoft Windows Event Log Monitor
- Microsoft Windows Performance Counter Monitor
- Microsoft Windows Resources Monitor
- Oracle 9i Application Server Monitor
- Oracle 10g Application Server Monitor
- Ping Monitor
- Script Monitor
- Service Monitor
- SNMP Monitor
- SNMP Trap Monitor
- UDDI Monitor
- URL Monitor
- URL Content Monitor
- URL List Monitor

- URL Sequence Monitor
- Web Script Monitor

### **Monitors Tested for UNIX Operating Systems**

- CPU Monitor
- Database Query Monitor
- Disk Space Monitor
- Log File Monitor
- Port Monitor
- Script Monitor
- Service Monitor
- UNIX Resources Monitor
- URL Monitor
- URL Content Monitor
- URL Sequence Monitor

## Troubleshooting and Limitations

This section contains troubleshooting and limitations for the following issues relating to working with SiteScope in an internationalization environment.

- “General Limitations for Using SiteScope in an I18N Environment” on page 1552
- “Database Environment Issues” on page 1553
- “Troubleshooting Remote UNIX Servers Not Configured For an English Locale” on page 1553

### **General Limitations for Using SiteScope in an I18N Environment**

- User name, password, and URLs must be in English characters.
- Support for internationalization is available only in the new user interface.
- The machine on which SiteScope is installed (SiteScope machine) and the monitored machine must have the same locale. English is the default locale.
- The SiteScope machine can have a non-English locale in addition to English. For example, the monitored machine supports the German locale while the SiteScope machine supports German and English. For details on setting a non-English locale, see “Configure SiteScope for a Non-English Locale” on page 1547.
- When deploying the Web Script Monitor, script names and transaction names must also be in English characters.
- Script monitor on Redhat ES4 does not support parameters in any language other than English.



- ▶ SiteScope always uses "en\_US" locale for parsing dates retrieved from remote UNIX machines (for example, during a File monitor run). If the UNIX machine's default locale is different from en\_US, in the definition of the UNIX remote for this machine, the **Initialize Shell Environment** field must contain "LANG=C; export LANG".
- ▶ The WMI implementation in SiteScope is supported for machines with an English locale only (both monitored machines and SiteScope server machine).

### **Database Environment Issues**

- ▶ When you create a new Oracle instance in an Oracle database, you must specify the character set for the instance. All character data, including data in the data dictionary, is stored in the instance's character set.
- ▶ The Database Query Monitor can connect to an Oracle database but the Oracle user names and passwords must contain only English characters.

### **Troubleshooting Remote UNIX Servers Not Configured For an English Locale**

#### **Problem:**

The File Monitor and Directory Monitor may fail when using UNIX remote servers that are not configured by default for an English locale or language.

#### **Resolution:**

Add "LANG=C; export LANG" to the **Initialize Shell Environment** property of the problematic UNIX remote server.



# **Part VII**

---

## **Templates**



---

## SiteScope Templates

This chapter includes the main concepts, tasks, and reference information for SiteScope templates.

### **This chapter includes:**

#### **Concepts**

- SiteScope Templates Overview on page 1558
- Understanding Templates on page 1561
- Template Examples on page 1564
- Planning Templates on page 1565
- Working with Template Variables on page 1567
- Counter Selection in Monitor Templates on page 1573
- Deploying a Template Using a CSV File on page 1577
- Updating Template Deployments on page 1578

#### **Tasks**

- Configure a SiteScope Monitoring Solution Using a Template – Workflow on page 1580
- Publish Template Updates to Related Group Deployments on page 1596
- Modify Counter Selection Strings to Use Regular Expressions on page 1601
- Export and Import a Template on page 1602

#### **Reference**

- Reserved Template Group Types on page 1603
- SiteScope Templates User Interface on page 1604

## SiteScope Templates Overview

You use templates to rapidly deploy sets of monitors that check systems in the infrastructure that share similar characteristics.

SiteScope provides three types of templates: user-defined templates, Monitor Deployment Wizard templates, and predefined solution templates. This chapter discusses user-defined templates. For information on Monitor Deployment Wizard templates, see “Monitor Deployment Wizard Templates and Variables” on page 1816. For information on predefined solution templates, see “SiteScope Solution Templates” on page 1665.

Advantages of using SiteScope user-defined templates include:

- ▶ You can create and customize your own templates to meet the requirements of your organization.
- ▶ SiteScope templates are used to standardize a set of monitor types and configurations into a single structure. This structure can then be repeatedly deployed as a group of monitors targeting multiple elements of the monitored environments.
- ▶ Templates provide an enterprise solution for standardizing the monitoring of the different IT elements in your enterprise, including servers, applications, databases, network environments, and so forth.
- ▶ Templates speed the deployment of monitors across the enterprise through the single-operation deployment of groups, monitors, alerts, remote servers, and configuration settings.
- ▶ Templates provide the ability to view how the actual monitored deployments comply with the standardized deployment as defined in the template. This ensures that any changes in the monitored environment can be quickly updated in the monitoring infrastructure and that the monitoring infrastructure is still compliant with the standards set in the template.

- ▶ You can use silent template deployment to submit deployment requests, and continue to use SiteScope without having to wait for the template deployment process to finish. The template deployment requests are queued and processed in the background. If SiteScope restarts before all requests in the queue are complete, it automatically continues the deployment process after the restart.
- ▶ The Publish Template Changes Wizard provides the ability to make changes to the template, and publish the changes to all SiteScope objects deployed by the template. If a change is required to a template object, for example, a threshold value changes or a new monitor or alert is required, you can update the template once and publish the changes to all deployed groups without having to update each object individually.

## Template Elements and Features

You create templates within a template container in the template view. These elements are then displayed in the template tree where you can access them for changes or deployment. For more information, see “Understanding Templates” on page 1561.

You use templates to deploy a standardized pattern of monitoring to multiple elements in your infrastructure. Effective development and use of templates requires some planning because you can add multiple objects types to the template. For more information, see “Planning Templates” on page 1565.

You create a template by adding and configuring groups, remote server definitions, monitors, alerts, and variables to the template. You use template variables as substitution markers for configuration settings that you want to change dynamically or interactively each time you deploy the template. Creating and referencing variables is an action that is unique to templates. For more information, see “Working with Template Variables” on page 1567.

Several SiteScope monitor types use a measurement counter browser function to dynamically query applications and systems for the metrics that are available for monitoring. When you create one of these monitors manually, you use a multiple step procedure to view and select counters. An alternative method is used to select counters when deploying templates. For details, see “Modify Counter Selection Strings to Use Regular Expressions” on page 1601.

After you create and configure templates, you deploy them in the SiteScope hierarchy. For details on deploying templates, see “Deploy the Template” on page 1585. If you subsequently want to make changes to the source template, you can automatically publish the changes to SiteScope objects deployed by the template using the Publish Template Changes Wizard. For details on updating templates, see “Updating Template Deployments” on page 1578.

---

**Note:** For information on configuring internal properties in SiteScope templates, refer to the HP Software Self-solve knowledge base ([h20230.www2.hp.com/selfsolve/documents](http://h20230.www2.hp.com/selfsolve/documents)). To enter the knowledge base, you must log in with your HP Passport ID.

---



## Understanding Templates

Templates are objects you use to reproduce groups, servers, monitors, and alerts according to a predefined pattern and configuration. You can deploy all of the items defined in the template in a single operation by copying the template to a location in the SiteScope hierarchy. Templates also use template variables that you use to interactively set certain monitor, server, and alert configuration settings when you deploy the template. Once you have created a template, you can use it to deploy monitors as often as needed.

The following methods are used for adding configurations to the created template.

- ▶ Copy an existing group and monitor hierarchy from a SiteScope to the template and edit the elements for use as a template. For details, see “Create a Template by Copying Existing Configurations” on page 1586.
- ▶ If there are no applicable SiteScope monitor elements in your enterprise or if you want to create new objects or settings, you can manually create template groups, monitors, servers, and alerts in the template. For details, see “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580.

---






### Tip:



- ▶ If SiteScope monitoring has not yet been configured and you are not familiar working with SiteScope monitors and groups, you should set up some sample groups, monitors, and alerts before you create templates. This helps familiarize you with the monitor configurations and the relationship between monitors, groups, and alerts. Afterwards, you can copy the structure from the SiteScope and convert the configurations to a template.
  - ▶ To help you get started with templates, SiteScope provides example templates for monitoring in Windows and UNIX environments. For details, see “Template Examples” on page 1564.
-

## Template Objects

Templates are created and stored in a template container in the template tree. The template variable definitions and SiteScope objects configurable using the template are displayed as objects within the template.

The following table describes the objects used in templates:

Icon	Object Type	Description
	Template Container	A template container enables you to manage your template monitoring solutions. You can add a template to a template container only. For details on configuring this object, see “New Template Container Dialog Box” on page 1609.
	Template	The template contains the SiteScope group, monitors, remote servers, variable definitions, and alerts that make up the template monitoring solution. For details on configuring this object, see “New Template Dialog Box” on page 1611.
	Template Variable	A variable is used to prompt for user input during template deployment. Template variables are either user-defined or predefined system variables. For details on configuring this object, see “New Template Variable Dialog Box” on page 1613.
	Template Remote Server	A template remote server is used to define Windows or UNIX remote server preferences that are created when the template is deployed. For details on configuring this object, see “New Template Remote Server Dialog Box” on page 1615.
	Template Group	A template group contains the template monitors and associated alerts. You use template groups to manage the deployment of monitors and associated alerts in your infrastructure. For details on configuring this object, see “New Template Group Dialog Box” on page 1617.

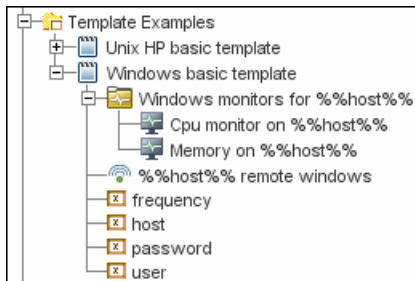
Icon	Object Type	Description
	Template Monitor	Template monitors are used to define monitors that are created when the template is deployed. For details on configuring this object, see “New Template Monitor Dialog Box” on page 1620.
	Template Alert	Template alerts are used to define alerts on groups and monitors that are created when the template is deployed. If an alert has been set up for the template monitor or group, the alert symbol is displayed next to the monitor or group icon. For details on configuring this object, see “New Template Alert Dialog Box” on page 1622.

## Template Examples

SiteScope provides template examples for monitoring in Windows and UNIX environments. These templates are available from the **Template Examples** folder in the template tree. You can use the template examples to help familiarize you with using SiteScope templates. Amongst other things, you can use it to see the following:

- ▶ How template groups, monitors, and remote servers are used
- ▶ The connection between the template remote server and the monitor using it
- ▶ Variable value usage and system variable usage

The following example shows the **Windows basic template**. The template contains a template group, **Windows monitors for %%host%%**, two template monitors (CPU and Memory), four user-defined variables (host, user, password, and frequency), and a template remote server.



## Planning Templates

Template planning is important for effective SiteScope management. You should consider the group and monitor relationships and properties in the template structure and how it fits into the overall monitoring environment.

The following are things to consider as you plan templates:

Object	Consideration
<b>Variable properties</b>	Decide which monitor configuration properties vary from one template deployment to another. For example, the target server address or resource to be monitored is a common variable property. You should also consider what naming conventions you want to use for groups and monitors. You use template variables to enter or select values for variable properties each time you deploy the template. Not all monitor configuration properties can be configured using variables. For more information, see “Working with Template Variables” on page 1567.
<b>Servers</b>	Decide which servers are the target servers. This is where the objects being monitored are located. Template servers are replicated automatically when the template is deployed. You can also define them manually in the Microsoft Windows Remote Servers or UNIX Remote Servers container of the remote server tree. For more information, see “Remote Servers Overview” on page 1276.
<b>Monitor types</b>	Decide which monitor types you want to replicate using templates. These should be monitor types that monitor multiple systems. For example, CPU, Disk, Memory and Service monitor types are commonly deployed for each server in the infrastructure. You can also include multiple instances of the Service Monitor type in a template to monitor different services or processes running on each server.

Object	Consideration
<b>Common properties</b>	For configuration properties that should be the same from one template deployment to another, you must decide what the values should be. For example, the <b>Frequency</b> setting is a required setting for each monitor type. The default setting is 10 minutes. Depending on what is to be monitored and the overall monitor load, you may want to change this value so that monitors created using the template run more often.
<b>Group structure</b>	Decide the group structure you want to use to organize the monitors. The organization groups and monitors in the template should be compatible with your overall plan for organizing the monitoring in your environment. The group structure you use may affect reporting, alerting, and monitoring.
<b>Alerts</b>	Decide if you want to deploy alerts as part of the template. Consider which alert types and actions you want to associate with the templates and monitors. Alerts deployed as part of a template have their <b>Alert Targets</b> property set to all monitors defined in the template (see “SiteScope Alerts Page” on page 1997). For example, a template alert added to a template group alerts on any monitor belonging to that group. If this does not fit your alerting plan, you must edit the alert configuration after deployment or add alerts manually.

## Working with Template Variables

While you can create templates without using template variables, the use of variables is central to the power and utility of templates. Template variables are substitution markers for monitor configuration settings. You create template variables to represent monitor configuration settings that you want to be able to modify whenever you deploy the template. You reference the variable in a text box in one or more template monitors.

Examples of common uses for template variables are:

- server or host addresses
- disk drive designators
- file paths
- monitor name descriptions

This is an overview of the steps required to enable template variables:

### **1 Create the template variable in the template.**

For more information on the user interface, see “New Template Variable Dialog Box” on page 1613.

### **2 Reference the variable in one or more configuration objects in the template.**

For more information on this topic, see “Referencing Template Variables” on page 1571.

Each variable that is referenced in a monitor or group object in a template prompts the display of a corresponding entry box when the template is deployed. The variable name is used as a label for the text entry box.

Some monitor configuration settings cannot be set using template variables. With the exception of the remote server selection menu, configuration items that are normally selected using a selection drop-down cannot be defined using template variables. Configuration items that are normally selected using a check box or radio selection cannot be configured using template variables.

Template variables are always child elements of the template container in which they reside. Variables can be referenced and used to define configuration settings for group, monitor, or alert configuration templates within the template. For information about the types of template variables in SiteScope and the specific syntax conventions, see “Variable Syntax” on page 1568.

You should plan and create the template variables before you create other template objects, such as servers and monitors. This enables you to enter the references to the variables into the template monitors, groups, or alerts as you add them to the template. Deleting a template variable that has already been referenced in a template object requires that the referencing object be deleted from the template to clear the broken reference.

---

**Tip:** You can see examples of variables used in templates in the **Template Examples** in the template tree. For details, see “Template Examples” on page 1564.

---

This section contains the following topics:

- “Variable Syntax” on page 1568
- “Referencing Template Variables” on page 1571

### **Variable Syntax**

The following types of template variables are available in SiteScope:

- **User-defined variables.** They are used to enter text-based values during template deployment. User-defined variables must have the "%%" symbol either side of the variable name.
- **System variables.** A set of predefined variables you use to access both the list of remote servers known to SiteScope and system time information. System variables must have the "\$\$" symbol either side of the variable name.

Each type of variable has specific syntax conventions which are described in the following sections.



## Syntax for User-Defined Variables

User-defined template variables can contain only alphanumeric characters and the underscore character. You can create as many variables as you need.

Examples of valid template variable syntax are:

```
description_text
DiskDrive
TARGET_URL
matchExpression
```

You should choose variable names that describe the configuration parameter that is represented. The variable name is used as a label for the variable entry box on the variable value entry window when you deploy the template.

## Syntax for System Variables

SiteScope recognizes several pre-defined template variables. These are values that are known by the system, including the list of servers for SiteScope, detected servers such as NetBIOS, and user-defined server connection profiles such as remote UNIX. The syntax and description for the pre-defined system variables are:

Syntax for System Variables	Description
\$\$SERVER_LIST\$\$	Returns a list from which to select one of all the servers known by the platform. Use this to enable selection of remote servers for <b>Server</b> or <b>Host Name</b> properties only.
\$\$SERVER_NAMES\$\$	Derived from the \$\$SERVER_LIST\$\$ variable. Returns the name of the current server with \\ (backslashes) before the name. Use when referencing the server in other boxes.

Syntax for System Variables	Description
<p><code>\$\$SERVER_NAME_BARE\$\$</code></p>	<p>Derived from the <code>\$\$SERVER_LIST\$\$</code> variable. Returns the name of the current server without \\ (backslashes) before the name. Use when referencing the server in a box requiring just the name of the server (for example, when deploying CPU monitors or when referencing the name of the server in a description: "Disk space on server Mail.")</p>
<p><code>\$\$DATE\$\$</code></p>	<p>Returns the system date on the server where SiteScope is running. Use to add the date that a monitor was created to a name or description.</p>
<p><code>\$\$TIME\$\$</code></p>	<p>Returns the system time on the server where SiteScope is running. Use to add the time that a monitor was created to a name or description. The value represents the time that the template is actually deployed.</p>

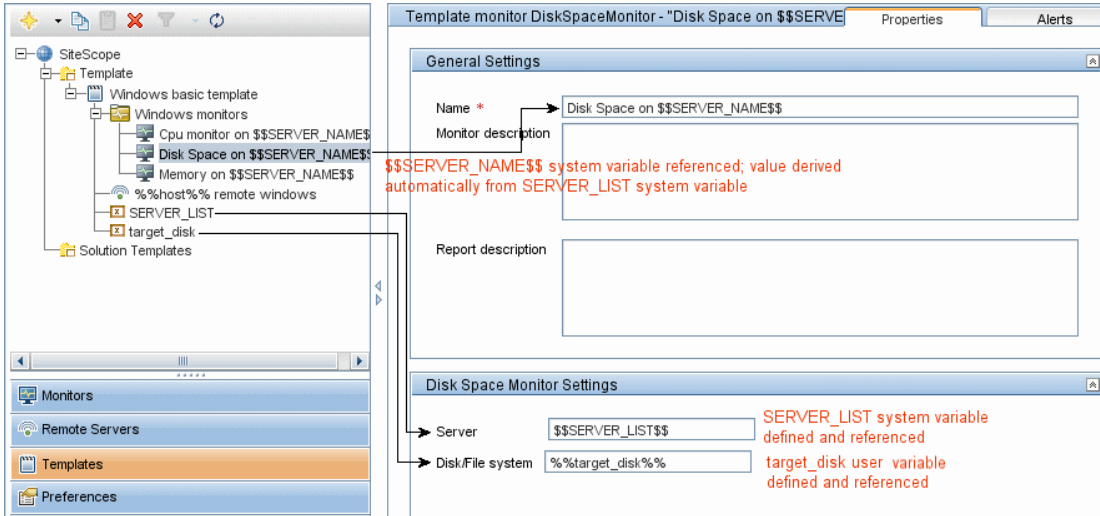
## Referencing Template Variables

After you have added template variables to a template, you must create references to them in a monitor or group configuration object. The syntax you use to reference a variable depends on the type of variable.

Variable Type	Syntax	Information
User-Defined	%%variable_name%%	<p>The reference is case sensitive and syntax sensitive.</p> <p><b>Note:</b> User-defined template variables must be created before they can be referenced in monitor or group configuration templates. Using the %% symbols with a text string that has not already been added to the template as a template variable does not create a reference to a template variable even if a matching variable name is added later.</p>
System	\$\$VARIABLE_NAME\$\$	<p>The reference is case sensitive and syntax sensitive.</p> <p>The \$\$SERVER_LIST\$\$ variable must be defined explicitly as a variable in the template. After this variable is defined, the \$\$SERVER_NAME\$\$ and \$\$SERVER_NAME_BARE\$\$ variables may be used in configuration objects by referencing them using the \$\$VARIABLE_NAME\$\$ syntax directly in the monitor or group configuration object.</p> <p>The \$\$TIME\$\$ and \$\$DATE\$\$ variables can also be referenced directly.</p> <p>For information about system variables, see “Variable Syntax” on page 1568.</p>

### Example - Referencing User-Defined and System Variables

The following shows examples of how to reference user-defined variables and the `$$$SERVER_LIST$$$` and the derived system variables for a monitor template.



## Counter Selection in Monitor Templates

SiteScope includes a number of application monitor types that are designed to monitor measurements specific to the target system. These browsable counter monitor types use a **Get Counters/Measurements** browser function in the Monitor Settings panel. Configuring these monitor types manually requires the following steps after selecting the monitor type:

- ▶ Specifying connection properties to the target system and then requesting that SiteScope retrieve the measurement counters from the remote system.
- ▶ Selecting the desired counters to be monitored and adding them to the configuration. After this, the monitor can be added to SiteScope.

Deploying monitors using templates does not accommodate a separate step for counter selection. Another mechanism is used to enable the selection of counters for these monitor types using templates. SiteScope uses text matching or regular expression matching to automate the counter selection step for template deployment. You use a counter selection step when you create the template monitor.

The simplest method for counter selection in templates is to select the specific counters explicitly in the monitor template. This creates an explicit text match used to select the matching counter during deployment. For information about the steps required to add a browsable counter monitor type with explicitly selected counters, see “Add Monitors to a Template” on page 1587.

If the specific counters on the target system vary from one deployment to another, you may be able to use a regular expression to match a pattern that represents the type or category of counter you want to monitor. For more information, see below.

This section contains the following topics:

- ▶ “Modifying Counter Selection Strings to Use Regular Expressions” on page 1574
- ▶ “Counter Selection Using Regular Expressions” on page 1574

## Modifying Counter Selection Strings to Use Regular Expressions

You can modify counter selection strings for template monitors to use regular expressions when you create the monitor, or you can edit the monitor later. For more information on modifying a template monitor for regular expression counter matching, see “Modify Counter Selection Strings to Use Regular Expressions” on page 1601.

### Counter Selection Using Regular Expressions

Many applications have a number of measurement counters that vary according to the system on which it is running, the configuration of system options, and the components installed. In this case, selecting explicit counters in a monitor template may not be useful across multiple instances of an application or system. Some systems have measurement counters that have a similar pattern but may vary by the name of a node or object context. You can use regular expressions in monitor templates to help automate the selection of multiple measurement counters.

---

**Note:** Use of this regular expression counter matching function requires knowledge of the counters on the system to be monitored. You should manually set up a monitor of the type you want to add to the template and carefully review the counters available on the type of system you want to monitor. Creating a "greedy" regular expression that matches large numbers of counters on a remote system may adversely affect SiteScope performance.

---

The steps you use to create a template monitor to use regular expressions are very similar to the procedure described in the previous section. Instead of selecting all of the counters to be monitored explicitly, you select one or more counters that are representative of all the counters you want to select. The counter selections in monitor templates are stored as text strings. You edit these strings to create patterns that SiteScope uses to find matching counters that are selected when the monitor is deployed.

### Examples - Using Regular Expressions

- **Example 1.** The following is a simple example of how a regular expression can be used for counter selection for a SNMP by MIB Monitor type in a template:

You want to monitor the following three counters from several SNMP agents in your infrastructure:

```
iso/org/dod/internet/mgmt/mib-2/system/sysDescr  
iso/org/dod/internet/mgmt/mib-2/system/sysUpTime  
iso/org/dod/internet/mgmt/mib-2/system/sysName
```

You could select all three counters explicitly in the template monitor. Alternately, you could select one of these and then modify the counter string to be a regular expression such as the following:

```
/isoVorgVdodVinternetVmgmtVmib-2VsystemVsys[DUN][a-zT]*/
```

In this example, the counter selection string has been edited to add a pair of / slashes before and after the string. This is necessary to indicate that the string is to be interpreted as a regular expression. Because the selection string included several / slash characters initially, each of these characters must be escaped by adding a \ backslash character immediately preceding it. The [DUN][a-zT]\* string includes two character class declarations commonly used in regular expression syntax. For more information on regular expression syntax, see “Using Regular Expressions” on page 261.

- **Example 2.** The following is an example of how a regular expression can be used for counter selection for a UNIX Resource Monitor type in a template:

You want to monitor daemon processes running on several UNIX or Linux servers in your infrastructure. The list of processing running might include the following:

```
Process\bash\NUMBER RUNNING
Process\./java/bin/java\NUMBER RUNNING
Process\.ns-admin\NUMBER RUNNING
Process\.ns-proxy\NUMBER RUNNING
Process\.ns-sockd\NUMBER RUNNING
Process\bin/sh\NUMBER RUNNING
Process\etc\init\NUMBER RUNNING
Process\usr/apache/bin/httpd\NUMBER RUNNING
Process\usr/lib/nfs/statd\NUMBER RUNNING
Process\usr/lib/saf/sac\NUMBER RUNNING
Process\usr/lib/saf/ttymon\NUMBER RUNNING
Process\usr/lib/snmp/snmpdx\NUMBER RUNNING
Process\usr/lib/ssh/sshd\NUMBER RUNNING
...
```

You can create a regular expression counter selection string to match only those processes that end with the letter "d". The following is an example regular expression to match this pattern:

```
/Process[\\Ww]{5,18}d[\\W]{1,2}NUMBER RUNNING/
```

As with Example 1, the counter selection string includes / slashes before and after the string to indicate that the string is a regular expression. The example process strings on the UNIX server include combinations of \ back slash and / forward slash characters. Because these characters have special meaning in regular expressions, they would have to be escaped. This can be complicated because the process strings have many variations and combinations of these and other symbols. The example regular expression used here simplifies the expression by using character class declarations. The [W] class is used to match punctuation marks. This matches on the \, -, :, and / characters that appear in some of the process strings without the need to escape the characters individually. For more information on regular expression syntax, see “Using Regular Expressions” on page 261.



## Deploying a Template Using a CSV File

After you create and configure templates, you deploy them in the SiteScope hierarchy. You can deploy templates directly from the user interface (see “Deploy a Template Using the User Interface” on page 1590), or you can deploy templates from an external Comma Separated Value (CSV) file. The CSV file is used to deploy the variable values defined in the template.

Advantages of using SiteScope CSV template deployment include:

- ▶ It is better suited than the user interface for performing mass deployments, since it is easier to enter and update all the template variable values in one CSV file.
- ▶ You can perform multiple deployments at one time, without having to manually enter variable values for each deployment in the user interface.
- ▶ The template is deployed silently (the template deployment request is submitted to a queue and the deployment is handled in the background). This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent\_deployment.log**.

---

**Note:** The maximum queue length for silent deployment is 2000 (each line in a CSV file represents one deployment in the queue).

---

For details on how to perform this task, see “Deploy a Template Using a CSV File” on page 1592.

## Updating Template Deployments

Using the Publish Template Changes Wizard, you can view how the actual monitored deployments comply with the standardized deployment as defined in the template. This ensures that any changes in the monitored environment can be quickly updated in the monitoring infrastructure and that the monitoring infrastructure is still compliant with the standards set in the template.

---

**Note:** You can run the Publish Template Changes Wizard provided you have **Edit groups** permissions, and only on groups for which you have permissions in the **Allowed groups** list. Any deployed groups that are not in your allowed groups list are not displayed in the wizard.

---

When you deploy a template, the deployed parent group is automatically associated to the template. If you subsequently make changes to the template, you can automatically publish the changes to SiteScope objects deployed by the template using the Publish Template Changes Wizard. The wizard enables you to update related deployed groups across the enterprise whenever the template is updated without having to update each object individually. A deployed group consists of the groups, monitors, alerts, variables, and the remote server configured in the template. For details on how to deploy a template, see “Deploy the Template” on page 1585.

The Publish Template Changes Wizard enables you to update deployed groups in the following ways:

- ▶ You can publish only the changes in the template to the deployed groups. This would create added objects and update values of existing objects, but leave other objects not in the template intact.
- ▶ You can publish the changes in the template to the deployed groups and have SiteScope make the above changes and delete all other SiteScope objects from the group that are not in the template groups.

For details on how to publish template changes, see “Publish Template Updates to Related Group Deployments” on page 1596.

For details on the Publish Template Changes Wizard user interface, see “Publish Template Changes Wizard - Select Deployed Groups Page” on page 1626.

## Notes and Limitations

- ▶ If you are using groups deployed by templates created in versions of SiteScope earlier than 9.50, root groups are not associated with the source template. You can update these template deployments using the following methods:
  - ▶ Manually associate the template groups with the source template using Global Search and Replace.
  - ▶ Enter the path of the source template in the **Source template** box in the General Settings for the current group.
- ▶ Templates and deployed groups are internally linked by an ID. This means that you can publish changes even if the name of the template or the root group in a deployed group have changed.
- ▶ For changes to be published, all changes in the root group hierarchy must succeed. If any changes to a group fail, all changes to that group are rolled back.
- ▶ The Publish Template Changes Wizard does not support regular expressions in threshold settings.
- ▶ The Publish Template Changes Summary report PDF is not supported in Firefox 2.x.
- ▶ Properties are displayed in the Publish Template Changes Wizard according to the locale of the server where SiteScope is installed. The browser locale has no effect on how the properties are displayed.
- ▶ You cannot replace an existing monitor target server using the Publish Template Changes wizard or auto deployment update (see “Publishing Template Changes Using the XML” on page 1650), although you can change property values of the target server itself, if required.

- ▶ To publish changes in browsable monitor counters to deployed groups, there must be a connection to the remote server on which the monitor groups are deployed.

## **Configure a SiteScope Monitoring Solution Using a Template – Workflow**

This task describes the steps for creating a SiteScope monitoring solution using a template. To view a flowchart of this task, see “Configure a SiteScope Monitoring Solution Using a Template – Flowchart” on page 51.

---

### **Tip:**

- ▶ We recommend that you create template objects in the order listed. You can skip the steps for any template objects that you do not require.
- ▶ To help you get started with templates, SiteScope provides example templates for monitoring in Windows and UNIX environments. For details, see “Template Examples” on page 1564.
- ▶ Some fields that contain drop-down lists when configuring objects in normal mode, are displayed as text boxes when configuring the object in template mode.

---

This task includes the following steps:

- ▶ “Prerequisites” on page 1581
- ▶ “Create a Template Container” on page 1581
- ▶ “Create a Template” on page 1581
- ▶ “Create Template Variables” on page 1582
- ▶ “Create a Template Remote Server” on page 1582
- ▶ “Create a Template Group” on page 1583
- ▶ “Create Template Monitor Instances” on page 1584

- “Set Up Monitor and Group Alerts” on page 1585
- “Deploy the Template” on page 1585
- “Results” on page 1585
- “Set Up Monitor and Group Reports (in the Monitor View)” on page 1585
- “Publish Changes to the Monitoring Solution” on page 1586

## 1 Prerequisites

- Check that the post-installation administration tasks have been performed before configuring SiteScope for monitoring. For details on these tasks, see “Setup and Administration” on page 45.
- To deploy a template, regardless of its content, you must have edit permissions on the deployment target group. You do not need edit permissions on the template objects (monitors, remotes, and alerts).

## 2 Create a Template Container

Create a template container to enable you to manage your monitoring solution.

For details on the New Template Container user interface, see “New Template Container Dialog Box” on page 1609.

## 3 Create a Template

Add a template to the template container. This is the container for your monitoring solution, in which you create groups, monitors, remote server, variables, and alerts for the monitoring solution.

For details on the New Template user interface, see “New Template Dialog Box” on page 1611.

**Note:** You can also copy an existing group and monitor hierarchy from a SiteScope to the template and edit the elements for use as a template. For details on how to perform this task, see “Create a Template by Copying Existing Configurations” on page 1586.

---

#### **4 Create Template Variables**

You can create template variables in the template that enable you to specify a different name for an object every time that you deploy the template. Variables should be the first objects you create in a template, because they are referred to when you create groups, monitors, servers, and alerts.

For details on the New Template Variable user interface, see “New Template Variable Dialog Box” on page 1613.

#### **5 Create a Template Remote Server**

In the template, you can define a remote Windows or UNIX server where the monitored objects are located. A template monitor may run on servers that are defined by template servers at the time of template deployment or on servers defined manually in Remote Servers. Template servers are added to the remote server tree under Microsoft Windows Remote Servers or UNIX Remote Servers when the template is deployed.

For details on the New Template Remote Server user interface, see “New Template Remote Server Dialog Box” on page 1615.

---

**Note:** You can add only one remote server to a template. This does not apply to templates created in versions of SiteScope earlier than 9.50.

---

### Example

A Windows template remote server has been created with the name %%host%% remote windows.

The image shows two panels of a configuration window. The top panel, titled "General Settings", contains a "Name" field with the value "%%host%% remote windows" and an empty "Description" field. The bottom panel, titled "Main Settings", contains several fields and options: "Server: \*" with value "%%host%%"; "Credentials:" with two radio buttons: "Use user name and password" (selected) and "Select predefined credentials"; under "Use user name and password", "User name" is "%%User%%" and "Password" is "\*\*\*\*\*"; under "Select predefined credentials", "Credential profile" is empty; a "Trace" checkbox is unchecked; "Method: \*" is "NetBIOS"; and "Remote machine encoding:" is "Cp1252".

## 6 Create a Template Group

In the template, create a template group to make the deployment of monitors and associated alerts manageable and effective for your organization.

For details on the New Template Group user interface, see “New Template Group Dialog Box” on page 1617.

---

**Note:** A template can have only one template group directly under it (the parent group). This does not apply to templates created in versions of SiteScope earlier than 9.50.

---

## 7 Create Template Monitor Instances

- a** Select the monitor instances you want to add to the template group. For details on adding monitors to a template, see “Add Monitors to a Template” on page 1587.
- 

### Note:

- A template monitor can run on servers that are defined by template servers at the time of template deployment or on servers defined manually in the Remote Servers container of the remote server tree. Whichever is the case, the value in the **Server** box must match the host name of an actual server at the time that the template is deployed after values have been substituted for the template variables. If the server name does not match the host name of a real server, the monitor fails. To automatically retrieve the template remote server name (if one was created), select the **Use already configured template remote under current template** check box in the Monitor Settings field.
  - You can add monitor instances directly to the template entity if you select **Allow creation of template monitors directly under template entity** in **Preferences > Infrastructure Preferences > Template Settings**.
- 

- b** You can manually set thresholds for monitors by setting logic conditions that determine the reported status of each monitor instance. For details on the Threshold Settings user interface, see “Threshold Settings” on page 362.

**Note:** After deploying a template, you can also set thresholds for one or multiple monitors using a baseline. For details on how to set monitor thresholds using a baseline, see “Set Monitor Thresholds Using a Baseline” on page 327.

- c** You can build dependencies between groups and key monitors to help control redundant alerting. For details on this topic, see “Monitoring Group Dependencies” on page 307.



## 8 Set Up Monitor and Group Alerts

Create alerts to send notification of an event or change of status in some element or system in your infrastructure.

For details on how to configure alerts, see “Configure an Alert” on page 1984.

## 9 Deploy the Template

After creating a SiteScope monitoring template, deploy the template to a group.

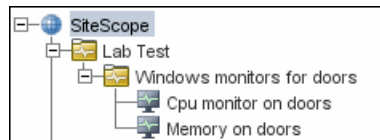
- ▶ You can deploy templates directly from the user interface. For details on how to perform this task, see “Deploy a Template Using the User Interface” on page 1590.
- ▶ Alternatively, you can deploy templates using a CSV file external to the SiteScope user interface. For details on this topic, see “Deploying a Template Using a CSV File” on page 1577. For details on how to perform this task, see “Deploy a Template Using a CSV File” on page 1592.

## 10 Results

SiteScope adds the groups, monitors, and alerts to the specified container in the monitor tree.

### Example

The template example, **Windows basic template**, was deployed to a group container named **Lab Test**. It contains a **CPU monitor** and **Memory monitor**, and was deployed to monitor resource usage on a server named **doors**.



## 11 Set Up Monitor and Group Reports (in the Monitor View)

Create reports to display information about how the servers and applications you are monitoring have performed over time.

For details on how to create reports, see “Create a Report” on page 2041.

## 12 Publish Changes to the Monitoring Solution

You can make changes to deployed templates, for example, by adding or removing monitors or modifying monitor properties. You do this by editing the template and using the Publish Template Changes Wizard to publish the changes to all the relevant objects deployed by the template.

For details on how to perform this task, see “Publish Template Updates to Related Group Deployments” on page 1596.



### Create a Template by Copying Existing Configurations

This task describes the steps involved in copying an existing group, monitor, or remote server from a SiteScope to the template and editing the elements for use as a template.

This task includes the following steps:

- “Copy an Existing Configuration to the Template” on page 1586
- “Edit Template Variables” on page 1586

### 1 Copy an Existing Configuration to the Template

Right-click the group, monitor, or remote server you want to copy, and select **Copy to Template**. In the Copy to Template Group dialog box, select the template group to which you want to add the copied configurations.

For details on the user interface, see “Copy to Template Tree Dialog Box” on page 379.

### 2 Edit Template Variables

If you are using template variables in the new template, edit each copied object by replacing the applicable configuration field’s value with the required variable syntax.

For details on this topic, see “Referencing Template Variables” on page 1571.

## **Add Monitors to a Template**

This task describes the steps involved in creating monitor templates.

This task includes the following steps:

- “Select the Monitor Type” on page 1587
- “Enter a Monitor and Host Name” on page 1587
- “Select Counters (for Monitors with Browsable Counters)” on page 1589
- “Configure the Monitor Settings” on page 1589

### **1 Select the Monitor Type**

Select the monitor type you want to configure for the template.

For details on the New Template Monitor user interface, see “New Template Monitor Dialog Box” on page 1620.

### **2 Enter a Monitor and Host Name**

Enter a monitor name of your choosing in the **Name** box (General Settings panel) and the host name in the **Server** box (Monitor Settings panel). If you are using template variables, enter the variable syntax for all fields whose values are to be replaced with a variable. This includes use of the `$$$SERVER_LIST$$` system variable.

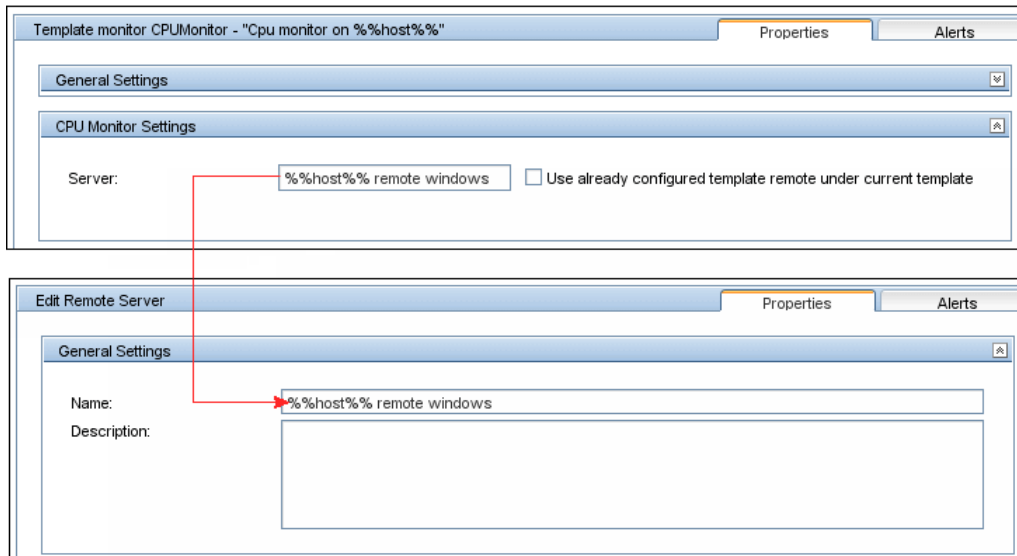
For details on this topic, see “Syntax for System Variables” on page 1569.

**Note:**

- ▶ If the monitor requires the remote server, enter the same value from the template remote server **Name** field in the **Server** box for the newly-created template monitor. These names must match for SiteScope to connect the newly-created remote server to the newly-created monitor. Alternatively, select the **Use already configured template remote under current template** check box to automatically retrieve the template remote name. For details on the New Template Monitor user interface, see “New Template Monitor Dialog Box” on page 1620.
- ▶ Do not use “\” in the monitor **Server** field, and in the remote server **Name** and **Server** fields.

**Example**

In this example, the template monitor (a SiteScope CPU monitor) is configured to run on the template remote server, %%host%% remote windows.



### 3 Select Counters (for Monitors with Browsable Counters)

Select counters for monitor types designed to monitor measurements specific to the target system.

- a** Click the **Get Counters** button, and select a server or enter the connection information for a server that is running the service or application that you want to monitor.
- b** Click the **Get Counters** button again to retrieve the available counters. The counter selection dialog box is updated.
- c** Select the measurements or counters that you want to monitor. If the specific counters on the target system vary from one deployment to another, you can use a regular expression to match a pattern that represents the type or category of counter you want to monitor. For details on how to perform this task, see “Modify Counter Selection Strings to Use Regular Expressions” on page 1601.

### 4 Configure the Monitor Settings

Configure the other monitor setting values as required in the Properties tab.

For details on the common monitor settings user interface, see “Common Monitor Settings” on page 354.

## **Deploy a Template Using the User Interface**

This task describes the steps involved in deploying a SiteScope template using the user interface.

---

### **Tip:**

- ▶ For mass deployments, you can also deploy templates using a CSV file. For details on deploying templates using a CSV file, see “Deploying a Template Using a CSV File” on page 1577.
  - ▶ You can also deploy and update the template using an XML file external to the SiteScope user interface. For details on this topic, see “Auto Template Deployment Overview” on page 1644.
- 

This task includes the following steps:

- ▶ “Prerequisites” on page 1590
- ▶ “Deploy the Template” on page 1590
- ▶ “Results” on page 1591

### **1 Prerequisites**

If you intend to deploy monitors to multiple servers at the same time, you must use a variable as the **Host** value for the template remote server. On deployment, specify multiple server names separated by commas (",") for the host variable.

### **2 Deploy the Template**

- a** After creating a SiteScope monitoring template, deploy the template to a group.
  - ▶ From the monitor tree, right-click the group into which you want to deploy the template, and select **Deploy Template**. In the Select Template dialog box, select the template you want to deploy. For details on the Select Template user interface, see “Select Template Dialog Box” on page 378.

- ▶ From the template tree, right-click the template you want to deploy, and select **Deploy Template**. In the Select Group dialog box, select a group into which you want to deploy the template. Alternatively, you can click the **New Group** button and create a new group to which you can deploy the template. For details on the Select Group user interface, see “Select Group Dialog Box” on page 1636.
- b** Enter the required variable values in the entry boxes displayed. The entry boxes displayed correspond to the template variables used in the template objects. For details on the user interface, see “Deployment Values Dialog Box” on page 1637.

### Example

If you deploy the **Windows basic template** from the **Template Examples** folder in the template tree to a SiteScope group, the following entry boxes are displayed in the Deployment Values input window.



The screenshot shows a window titled "Main Settings" with four input fields. The first three fields are empty, and the fourth field contains the value "600".

Host *	<input type="text"/>
User Name *	<input type="text"/>
Password *	<input type="text"/>
Frequency (sec) *	<input type="text" value="600"/>

### 3 Results

A summary of the template deployment is displayed. If the deployment is successful, the template objects are added to the monitor tree.

If a template deployment fails, a message displays reasons for the failure. A template monitor might fail to deploy, for example, in the case of a Disk Space monitor, if the disk drive specified in the template does not exist on the deployed server.

## Deploy a Template Using a CSV File

This task describes the steps involved in deploying a SiteScope template using a CSV file.

---

**Note:** To deploy a solution template using a CSV file, you must first make a copy of the solution template to a template container, and then make the changes required in the steps below to the copied template.

---

### Tip:

- ▶ You can also deploy templates using the user interface. For details, see “Deploy a Template Using the User Interface” on page 1590.
  - ▶ You can also deploy and update the template using an XML file external to the SiteScope user interface. For details on this topic, see “Auto Template Deployment Overview” on page 1644.
- 

This task includes the following steps:

- ▶ “Prerequisites” on page 1592
- ▶ “Edit the Template Variable Display Order” on page 1593
- ▶ “Create the CSV File” on page 1593
- ▶ “Deploy the Template” on page 1594
- ▶ “Results” on page 1595

### 1 Prerequisites

Make sure that the template group name has a unique value in each deployment instance. You can do this by using a variable in the group name (for example, in the **Windows basic template** in **Template Examples**, the group name contains the %%host%% variable), and entering a different variable value in each deployment.



## 2 Edit the Template Variable Display Order

Update the display order for each variable in the template, so that the order starts from 0 (instead of 1). This is to ensure that the variables taken from the CSV file are displayed in the correct order on deployment.

---

**Note:** If there is no display order defined for the variables, the deployment fails.

---

## 3 Create the CSV File

Open a new text file, and perform the following:

- a** For each deployment instance, add a line that includes values for each variable necessary in the deployment, separated by a comma (","). Enter values in the order that they are set to be displayed in the **Display order in the template** field (starting from the variable with display order 0).

---

**Note:**

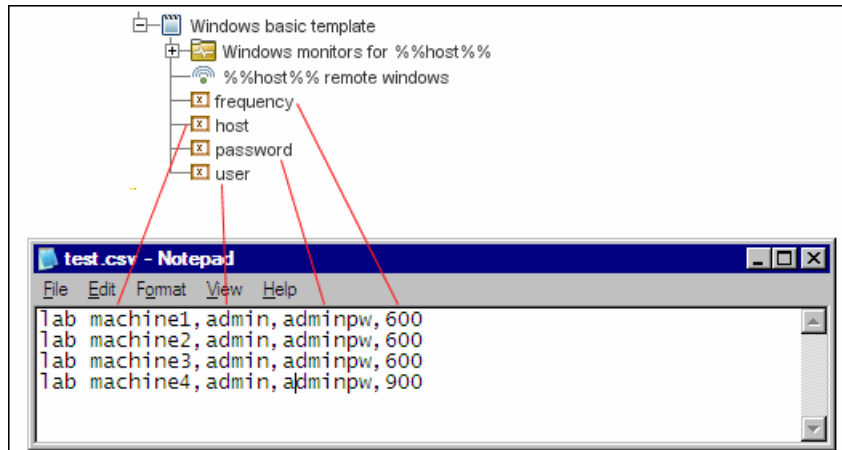
- Spaces are considered part of a field and should not be ignored.
  - You do not need to enter non-mandatory variables or default variable values in the CSV file. Instead, you should enter a comma followed by a comma (",,") to represent the variable value.
  - Passwords cannot be encrypted in the CSV file.
- 

- b** Save the file in CSV format. After the template is deployed, a group is created for each line in the CSV file.

**Example**

To deploy the **Windows basic template** using a CSV file, create a CSV file and enter host, user, password, and frequency values separated by a comma, for each deployment instance (this is the variable display order used in the template).

You do not need to enter a value in the CSV file for the **Frequency** variable (even though it is a mandatory variable), because a default value has been set for this variable in the template (provided you want to use the 600 seconds default value).

**4 Deploy the Template**

- a After creating a CSV file for the template, deploy the template to a group.
  - From the monitor tree, right-click the group into which you want to deploy the template, and select **Deploy Template Using CSV**. In the Select Template dialog box, select the template you want to deploy. For details on the Select Template user interface, see “Select Template Dialog Box” on page 378.
  - From the template tree, right-click the template you want to deploy, and select **Deploy Template Using CSV**. In the Select Group dialog box, select a group into which you want to deploy the template. Alternatively, you can click the **New Group** button and create a new group to which you can deploy the template. For details on the Select Group user interface, see “Select Group Dialog Box” on page 1636.

- b** In the Select CSV File dialog box, select the CSV file to use for template deployment. For details on the Select CSV File user interface, see “Select CSV File Box Dialog Box” on page 1639.

## 5 Results

If the deployment is successful, the template objects are added to the monitor tree. The monitor tree updates itself periodically. You can click the **Refresh** button in the tree toolbar to force an update to the monitor tree.

You can check the **silent\_deployment.log** file for a summary of the deployment.

For details of the log file, see “Log Files Page” on page 1954.

---

**Note:** Typed password values are not displayed in the log file, and instead of the real password, you see a sequence of asterisks ("\*\*\*\*\*").

---

## Publish Template Updates to Related Group Deployments

This task describes the steps involved in publishing template changes to related group deployments using the Publish Template Changes Wizard.

This task includes the following steps:

- “Run the Wizard” on page 1596
- “View the Structural and Content Differences” on page 1597
- “Add New Variable Values” on page 1599
- “Review the Publish Template Changes Results” on page 1600

### 1 Run the Wizard

In the template tree, right-click a template, and select **Publish Changes** to run the wizard. On the first page, select the related template groups that you want to update. You can also select the following options:

- **Enable delete on update** to delete SiteScope objects from the deployed groups that are not in the source template.
- **Verify template changes with remote servers** to verify the correctness of the monitor configuration changes in the selected template with the remote servers on which the template is deployed.

For details on the Publish Template Changes Wizard user interface, see “Publish Template Changes Wizard - Select Deployed Groups Page” on page 1626.

### Example - Select Deployed Groups Page

**Select Deployed Groups**

Select the groups that are associated with the deployed template to which you want to publish template changes.

SiteScope
 

- Lab Test
- Lab Test 1

Enable delete on update  
(Enables you to delete from the deployed templates, all SiteScope objects that are not in the so...)

## 2 View the Structural and Content Differences

View the structural differences between the template and the deployed groups. For details on the Review Compliancy user interface, see “Review Compliancy Page” on page 1627.

To view content differences in the template objects, click the **View Differences** link to open the Content Changes dialog box. This link appears only for template objects that have content differences. For details on the Content Changes user interface, see “Content Changes Dialog Box” on page 1629.

### Example - Review Compliancy Page

#### Review Compliancy

Displays the structural differences between the template and the deployed groups.  
If there are differences between the template and the deployed group object properties, you can click the View Differences link to display these differences.

**Total number of deployed groups for publishing changes: 4**  
**3 deployed groups with structural/content differences**

Group Name	Content Differences	
<ul style="list-style-type: none"> <li>[-] SiteScope\51\gr                             <ul style="list-style-type: none"> <li>cpu <a href="#">View Differences</a></li> <li>test - (Removed)</li> </ul> </li> </ul>		<input checked="" type="checkbox"/>
<ul style="list-style-type: none"> <li>[-] SiteScope\Windows monitor...                             <ul style="list-style-type: none"> <li>cpu <a href="#">View Differences</a></li> <li>test - (Removed)</li> </ul> </li> </ul>		<input checked="" type="checkbox"/>
<ul style="list-style-type: none"> <li>[-] SiteScope\Windows monitor...</li> </ul>		<input checked="" type="checkbox"/>

**1 deployed groups with no structural/content differences**

Group Name	Content Differences	
[-] SiteScope\gr\gr\gr		<input checked="" type="checkbox"/>

### Example - Content Changes Page

#### Content Changes

Review details of the content changes to be performed on the object's properties.

**Type : Monitor**  
**Name : Memory on DOORS**

Property Name	Current Value	Replacement Value	Action
Warning if	percentFull >= 93%warning every day, all...	percentFull > 80warning every day...	Ignored
Error if	percentFull >= 100%error every day, all day	percentFull >= 100%error	Ignored
Report topology ...	true		Deleted
Server	SiteScope Server	%%host%% remote windows	Modified
Baseline mode	Baseline activated	Monitor not selected for baselining	Ignored

### 3 Add New Variable Values

Add values for any new variables in the template. Variable values that are mandatory are indicated by a red asterisk (\*). You can also edit values of existing variables. Click **Apply** to complete the wizard and publish the template updates.

For details on the Modify Variables user interface, see “Modify Variables Page” on page 1631.

#### Example - Modify Variables Page

**Modify Variables**

Add values for new variables in the deployed group and/or edit existing variable values.

**Total number of deployed groups for publishing changes: 4**  
**3 deployed groups with missing variable values**  
 Enter missing variable values in the Variable Value box below.  
 A red asterisk indicates that the variable value is mandatory.

Variable Name	Variable Value	
[-] SiteScopeIS1lgr		<input checked="" type="checkbox"/>
[-] test*		
[-] freq*	600	
[-] SiteScopeIgrlgr		<input checked="" type="checkbox"/>
[-] test*		
[-] freq*	600	
[-] SiteScopeWindows monitor...		<input checked="" type="checkbox"/>

**1 deployed groups with existing variable values or with no variables**  
 Deployed groups with variables that have existing values or that have no variables are listed below.  
 You can expand groups that have variable values, and modify the variable values as required.

Variable Name	Variable Value	
[+] SiteScopeWindows monitor...		<input checked="" type="checkbox"/>

## 4 Review the Publish Template Changes Results

Review the results of the publish template changes and, if necessary, retry publishing the changes to the deployed groups that failed to update. For details on the Publish Results Summary user interface, see “Publish Results Summary Page” on page 1632.

Optionally, you can export the publish template changes results to a summary report (PDF file). For details on the summary report, see “Publish Template Changes Summary Report” on page 1633.

### Example - Publish Results Summary Page

#### Publish Results Summary

Displays a summary of the deployed groups affected by the template changes.  
Click the PDF report icon to review changes made to the deployed groups.

0 deployed groups were successfully updated.

1 deployed groups were not updated.



Root groups which were not changed:

Group Name	Reason
SiteScope\Windows monitors for labm1	
Cpu monitor on labm1	Monitor Cpu monitor on %%host%%frequency...
Memory on labm1	Monitor Memory on %%host%%frequency%...
Microsoft Windows Remote Servers	
labm1 remote windows	Monitor Memory on %%host%%frequency%...



## **Modify Counter Selection Strings to Use Regular Expressions**

This task describes the steps involved in modifying a template monitor to use a regular expression for measurement counter selection.

---

**Note:** This task applies to monitors with browsable counters only.

---

**To modify a template monitor for regular expression counter matching:**

- 1** In the template tree, click the monitor template you want to modify to open the template monitor Properties view.
- 2** Open the Monitor Settings pane, and in the **Measurements** or **Counters** section (depending on the monitor type), select a counter selection string that is representative of the pattern of counters you want to configure for the monitor, and click the **Edit** button for the counter string you want to edit. A string edit dialog opens.
- 3** Modify the counter selection string to be a regular expression by adding a slash ("/") character to the beginning and end of the string. Modify the string to use other pattern matching syntax as required. For more information on regular expression syntax, see “Using Regular Expressions” on page 261.



---

**Note:** If the template monitor was configured with explicit counter selections that can be matched using the regular expression that was entered, you can delete the extra counter strings by clicking the **Delete** button to the right of the counter string.

---



## **Export and Import a Template**

This task describes the steps involved in exporting and importing a template.

This task includes the following steps:

- “Export a Template” on page 1602
- “Import a Template” on page 1602
- “Result” on page 1602

### **1 Export a Template**

Right-click the template container object in the template tree that contains the template or templates you want to export, and click **Export**. Enter the name and location to which you want to save the template file and select the templates to export. For details on the Export Template user interface, see “Export Template Dialog Box” on page 1623.

### **2 Import a Template**

Once you have exported a template, you can copy the export file to another SiteScope server and import the template container object that contains the template or templates you want to use. Right-click the template container in the template tree into which you want to import the template or templates, and click **Import**. Enter the name and location of the file you want to import. For details on the Import Template user interface, see “Import Template Dialog Box” on page 1625.

---

**Note:** When importing templates to SiteScope that contain deprecated monitors from earlier version of SiteScope, the deprecated monitors are not displayed in the template tree.

---

### **3 Result**

Templates contained in the file are added to the template container. The imported templates can be used directly or modified as required.

## Reserved Template Group Types

The following table shows template types used by the SiteScope application. The templates in these directories are reserved, and are not used by alerts. For a list of templates used in alerts, see “SiteScope Alert Templates Directory” on page 1989.

---

**Note:** We do not recommend modifying the templates in these directories without following the specific procedures provided in the product documentation or as instructed by HP Software Support.

---

Template Group	Description	Location
MIB	Text used with SNMP traps	<SiteScope root directory>\templates.mib
Operating System	Shell commands to be run when monitoring remote UNIX servers	<SiteScope root directory>\templates.os
Performance Monitor	Used for NT performance monitoring	<SiteScope root directory>\templates.perfmon
Sound	Audio files used for sound alerts	<SiteScope root directory>\templates.sound
View	Query and XML/XSL templates	<SiteScope root directory>\templates.view

## SiteScope Templates User Interface




### **This section includes:**

- SiteScope Templates Page on page 1605
- Templates Tree - Properties Tab on page 1606
- Templates Tree - Alerts Tab on page 1607
- New Template Container Dialog Box on page 1609
- New Template Dialog Box on page 1611
- New Template Variable Dialog Box on page 1613
- New Template Remote Server Dialog Box on page 1615
- New Template Group Dialog Box on page 1617
- New Template Monitor Dialog Box on page 1620
- New Template Alert Dialog Box on page 1622
- Export Template Dialog Box on page 1623
- Import Template Dialog Box on page 1625
- Publish Template Changes Wizard - Select Deployed Groups Page on page 1626
- Select Group Dialog Box on page 1636
- Deployment Values Dialog Box on page 1637
- Select CSV File Box Dialog Box on page 1639
- Generate Auto Deployment XML on page 1640

## SiteScope Templates Page

<b>Description</b>	<p>Displays the name and description of the selected template container.</p> <p>Use this page to add template containers, or edit the properties of existing template containers (not Solution Templates).</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, select the <b>SiteScope</b> node.</p>
<b>Included in Tasks</b>	“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580
<b>Useful Links</b>	“Template Tree” on page 84

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Enables you to create a new template container. For details on the New Template Container user interface, see “New Template Container Dialog Box” on page 1609.
	Enables you to edit the selected template container.
	Deletes the template container.
<SiteScope Templates table>	Lists the predefined template that come with SiteScope (Template Examples, Monitor Deployment Wizard Templates, and Solution Templates), and any user-defined template containers. Double-click a template container to open the template container page for the selected template.
<b>Name</b>	The text name string assigned to the template container.
<b>Description</b>	A description of the template container that was assigned when creating or editing the template container.

## Templates Tree - Properties Tab

<b>Description</b>	<p>Displays the name and description of the selected template.</p> <p>Use this page to edit the properties of the template. In the template tree, select a template object (template group, template monitor, template variable) to display properties for the specific object.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand a template container and select a template. The Properties tab is displayed by default.</p>
<b>Included in Tasks</b>	“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580
<b>Useful Links</b>	“Template Tree” on page 84

### Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Name</b>	The template name.
<b>Description</b>	Enables you to add a description of the template.

## Search/Filter Tags






The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>
Add Tag	<p>Click to add a new keyword tag.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>

## Templates Tree - Alerts Tab

Description	<p>Displays a list of alerts associated with the solution template.</p> <p>Use this page to add, delete, or edit alerts associated with the template. In the template tree, select a template group or monitor to display alerts for the selected object.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, navigate to the group or monitor to which you want to view, add, or edit alerts. Click the <b>Alerts</b> tab.</p>
Included in Tasks	<ul style="list-style-type: none"> <li>➤ “Deploy a SiteScope Solution Template – Workflow” on page 1669</li> <li>➤ “Configure an Alert” on page 1984</li> </ul>
Useful Links	<ul style="list-style-type: none"> <li>➤ “Template Tree” on page 84</li> <li>➤ “SiteScope Alerts Page” on page 1997</li> </ul>


The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
	Click to open the New Alert dialog box, enabling you to define a new alert. For more details, see “New/Edit Alert Dialog Box” on page 1999.
	Click to open the Edit Alert dialog box, enabling you to edit the alert. For more details, “New/Edit Alert Dialog Box” on page 1999.
	Copies the alert.
	Pastes the alert.
	Deletes the alert.
<b>Name</b>	The text name string assigned to the alert definition.
<b>Status</b>	<p>The enabled/disabled status of the alert.</p> <ul style="list-style-type: none"> <li>▶ <b>Enabled.</b> Overrides any disable action on the alert and enables the alert for execution based on the conditions defined.</li> <li>▶ <b>Disabled indefinitely.</b> Prevents SiteScope from executing the alert action even if the alert condition is met until this radio button is cleared and the alert definition is updated.</li> <li>▶ <b>Disable on a one time schedule from &lt;Time1&gt; to &lt;Time2&gt;.</b> Prevents SiteScope from executing the alert action for the time period indicated, even if the conditions are met. The alerts are disabled at the beginning of the time period and re-enabled after the time period expires.</li> </ul>



GUI Element	Description
Description	A description of the alert definition that was assigned when creating or editing the alert.
Action Name	The name given to the action to be done when the alert is triggered. It is not the name of the alert.

## New Template Container Dialog Box

Description	<p>Enables you to define a new template container. You use template containers to store and manage templates. Template containers enable you to group and organize multiple templates in ways that describe their purpose or classification.</p> <p>Templates are displayed with the  icon in the template tree. Template containers can hold templates only.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click the SiteScope node or an existing template container, and select <b>Template Container</b>.</p>
Included in Tasks	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</p> <p>“Create a Template by Copying Existing Configurations” on page 1586</p>
Important Information	<p>Template containers can be added only to the SiteScope node in the template tree.</p>
Useful Links	<ul style="list-style-type: none"> <li>➤ “Understanding Templates” on page 1561</li> <li>➤ “Template Examples” on page 1564</li> <li>➤ “Template Tree” on page 84</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):


GUI Element	Description
<b>Name</b>	Enter a name for the template container. <b>Maximum length:</b> 250 characters
<b>Description</b>	Enables you to add a description for the template container.

## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>&lt;Tag name and values&gt;</b>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.  For details on using tags, see “Working with Search/Filter Tags” on page 107.
<b>Add Tag</b>	Click to add a new keyword tag.  For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.

 **New Template Dialog Box**

<b>Description</b>	<p>Enables you to add a template to a template container. An individual template is comprised of the object definitions of those objects that are created when the template is deployed.</p> <p>Templates are displayed with the  icon in the template tree. Templates can contain a group and subgroups, variables, and a remote server. They can also contain monitors, provided <b>Allow creation of template monitors directly under template entity</b> is selected in <b>Preferences &gt; Infrastructure Preferences &gt; Template Settings</b>.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click a template container, and select <b>New &gt; Template</b>.</p>
<b>Included in Tasks</b>	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</p> <p>“Create a Template by Copying Existing Configurations” on page 1586</p>
<b>Important Information</b>	<p>A template can have one template group only directly under it (the parent group). This does not apply to templates created in versions of SiteScope earlier than 9.50.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Understanding Templates” on page 1561</li> <li>➤ “Template Examples” on page 1564</li> <li>➤ “Template Tree” on page 84</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):


GUI Element	Description
<b>Name</b>	Enter a name for the template. The name you enter appears in the template tree as a child node of the template container. <b>Maximum length:</b> 250 characters.
<b>Description</b>	Enables you to add a description for the template.

## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>&lt;Tag name and values&gt;</b>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.  For details on using tags, see “Working with Search/Filter Tags” on page 107.
<b>Add Tag</b>	Click to add a new keyword tag.  For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.

## New Template Variable Dialog Box

<b>Description</b>	<p>Enables you to add a template variable to a template. A variable is used to enable prompting for user input during template deployment. Template variables are either user-defined or predefined system variables that provide access to the list of remote server connections known to SiteScope.</p> <p>Template variables are displayed with the  icon in the template tree.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click a template, and select <b>New &gt; Variable</b>.</p>
<b>Important Information</b>	<p>When configuring variables for <b>Frequency</b> and <b>Error frequency</b> in the Monitor Run Settings, the variable values can only be in time units of seconds.</p>
<b>Included in Tasks</b>	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Understanding Templates” on page 1561</li> <li>➤ “Working with Template Variables” on page 1567</li> <li>➤ “Template Examples” on page 1564</li> <li>➤ “Template Tree” on page 84</li> </ul>


## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Name</b>	<p>Enter a name for the template variable. The name you enter is used to identify the variable in the template in the template tree. This is the name that must be used when referring to the variable in other template objects.</p> <p><b>Note:</b> The name of a variable cannot be edited once the variable has been added. To change a variable name, delete the variable and create a new one with the correct name.</p>
<b>Display name</b>	<p>Enter a display name if you want a different name to be displayed instead of the variable name on deployment. You must still use the variable name when referencing the variable in a template object.</p>
<b>Description</b>	<p>Enter a description for the variable.</p>
<b>Default value</b>	<p>Enter a default value to be used for this variable. If you do not enter a value in this box and the box requires a value, you are prompted to enter a value when deploying the template.</p>
<b>Display order in template</b>	<p>Enter the variable display sequence number. This is the order in which SiteScope prompts you to enter values for a variable on deployment. Variables are displayed in ascending order. Variables that have no display number are displayed at the end.</p> <p><b>Note:</b> The display order does not change the order of the variables within the template definition.</p>

GUI Element	Description
<b>Password variable</b>	<p>If selected, hides the default value and the value entered during deployment.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> This option is automatically selected for any variable from previous versions of SiteScope that has a name ending with PASSWORD or password.</p>
<b>Mandatory variable</b>	<p>If selected, the variable field requires a value and prompts you to enter a value when deploying the template. To set a variable with a non-mandatory value, clear the check box. When this option is cleared, SiteScope uses an empty String ("") as a value for a non-mandatory variable.</p> <p><b>Default value:</b> Selected</p>

## **New Template Remote Server Dialog Box**

<b>Description</b>	<p>Enables you to create a UNIX or Windows remote server in the template. A template remote server is used to define remote server preferences that are created when the template is deployed.</p> <p>A template remote server is displayed with the  icon in the template tree.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click a template, and select <b>New &gt; Microsoft Windows/UNIX Remote Server</b>.</p>
<b>Included in Tasks</b>	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</p>


<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>➤ Enter the actual values for those fields that remain constant throughout the template deployment. Enter template variables in those fields whose values are replaced with a variable value when the template is deployed. For details, see “Referencing Template Variables” on page 1571.</li> <li>➤ You can add only one remote server to a template. This does not apply to templates created in versions of SiteScope earlier than 9.50.</li> <li>➤ You can add a new variable from the New Template Remote Server dialog box by clicking the <b>New Variable</b> button, and configuring the variable as described in “New Template Variable Dialog Box” on page 1613.</li> <li>➤ You cannot replace an existing monitor target server using the Publish Template Changes wizard or auto deployment update (see “Publishing Template Changes Using the XML” on page 1650), although you can change property values of the target server itself, if required.</li> <li>➤ Do not use “\” in the remote server <b>Name</b> and <b>Server</b> fields, and in the monitor <b>Server</b> field.</li> <li>➤ Some fields that contain drop-down lists when configuring objects in normal mode, are displayed as text boxes in template mode.</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ “Understanding Templates” on page 1561</li> <li>➤ “Remote Servers Overview” on page 1276</li> <li>➤ “Template Examples” on page 1564</li> <li>➤ “Template Tree” on page 84</li> </ul>

For a description of the elements found in the Microsoft Windows New Remote Server dialog box, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.

For a description of the elements found in the UNIX New Remote Server dialog box, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.



## New Template Group Dialog Box

<b>Description</b>	<p>Enables you to add a template group to a template or to a template group to create a subgroup. You use template groups to replicate monitoring deployment to multiple locations in the infrastructure.</p> <p>Template groups are displayed with the  icon in the template tree. A template group can contain monitors, alerts, and subgroups.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click a template or template group, and select <b>New &gt; Group</b>.</p>
<b>Included in Tasks</b>	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ A template can have only one template group directly under it (the parent group). This does not apply to templates created in versions of SiteScope earlier than 9.50.</li> <li>▶ By default, you can create template monitors, alerts, and subgroups in the parent group or in subgroups only. If you want to create template monitors directly under a template entity, select the <b>Allow creation of template monitors directly under template entity</b> check box in <b>Preferences &gt; Infrastructure Preferences &gt; Template Settings</b>.</li> <li>▶ You can add a new variable from the New Template Group dialog box by clicking the <b>New Variable</b> button, and configuring the variable as described in “New Template Variable Dialog Box” on page 1613.</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Understanding Templates” on page 1561</li> <li>▶ “Template Examples” on page 1564</li> <li>▶ “Template Tree” on page 84</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):


GUI Element	Description
<b>Group Name</b>	<p>Enter a name for the template group, preferably using a template variable. A template variable enables you to specify a different name for the group every time you deploy the template. If the group name does not include a variable, multiple deployments of the template in the same directory fail because the group name is not unique. For details on using template variables, see “Referencing Template Variables” on page 1571.</p>
<b>Group Description</b>	<p>Enables you to add a description for the template group. This can include the most common HTML tags for text styling, such as &lt;BR&gt;, &lt;HR&gt;, and &lt;B&gt;, and hyperlinks. The description is displayed only when viewing or editing the group’s properties in the Dashboard. For details on adding a hyperlink, see “Add URL Links to Group Description - Optional” on page 295.</p> <p><b>Note:</b> This field does not support Javascript/iframes/frames or other advanced features. HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line).</p>

## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>
<b>Add Tag</b>	<p>Click to add a new keyword tag.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>


## New Template Monitor Dialog Box

<p><b>Description</b></p>	<p>Enables you to add a template monitor to a template group or subgroup. Template monitors are used as the basis for the creation of actual monitors at the time that the template is deployed.</p> <p>Template monitors are displayed with the  icon in the template tree. By default, you can create template monitors only in a template group. To create template monitors directly under a template entity, select the <b>Allow creation of template monitors directly under template entity</b> check box in <b>Preferences &gt; Infrastructure Preferences &gt; Template Settings</b>.</p> <p>Template monitors can contain alerts.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click a template group, and select <b>New &gt; Monitor</b>. Select the monitor type you want to configure for the template.</p>
<p><b>Included in Tasks</b></p>	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</p>

<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>➤ Template monitors are not active monitor instances. Monitors are created and activated based on these template configurations only when you deploy the template.</li> <li>➤ You can create a new variable from this dialog box by clicking the <b>New Variable</b> button, and configuring the variable as described in “New Template Variable Dialog Box” on page 1613.</li> <li>➤ When selecting the server that you want monitor, you can use the template remote server (if one was created) without having to enter its name, by selecting the <b>Use already configured template remote under current template</b> check box.</li> <li>➤ Do not use "\\\" in the monitor <b>Server</b> field, and in the remote server <b>Name</b> and <b>Server</b> fields.</li> <li>➤ The Web Script monitor is not supported in templates.</li> <li>➤ When deploying a Script monitor from a template, the case of the remote script name must match that of the script name in the scripts subdirectory. Otherwise, the selected script is shown as 'none'.</li> <li>➤ The Network Bandwidth monitor's non-default thresholds are not copied properly to a template.</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>➤ “Understanding Templates” on page 1561</li> <li>➤ “Template Examples” on page 1564</li> <li>➤ “Template Tree” on page 84</li> </ul>

For a description of the elements found in the New Monitor page, see “New Monitor Page” on page 351.

## New Template Alert Dialog Box

<b>Description</b>	<p>Enables you to define alerts for a template group or a template monitor. Template alerts are used to define alerts on monitors that are created when the template is deployed.</p> <p>If an alert has been set up for the template group or monitor, the alert  symbol is displayed next to the group or monitor icon.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click a template group or template monitor, and select <b>New &gt; Alert</b>.</p>
<b>Included in Tasks</b>	<p>“Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</p>
<b>Important Information</b>	<p>You cannot select the <b>Disable or Enable Monitors</b> alert action when creating an alert template. Template alerts are enabled for all the monitors belonging to the object for which they were defined. For example, if an alert is defined for a monitor, then it is activated on that monitor only. If an alert is defined for a template, then it is activated for all the monitors in the template.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Understanding Templates” on page 1561</li> <li>➤ “Template Examples” on page 1564</li> <li>➤ “Template Tree” on page 84</li> </ul>

For a description of the elements found in the New Alert dialog box, see “New/Edit Alert Dialog Box” on page 1999.

## Export Template Dialog Box

<p><b>Description</b></p>	<p>Enables you to export templates for use in other SiteScope installations. This allows you to replicate standardized monitor configurations across the enterprise. After exporting, the template still remains in the template container.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click the template container object that contains the template or templates you want to export, and select <b>Export</b>.</p>
<p><b>Included in Tasks</b></p>	<p>“Export and Import a Template” on page 1602</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ SiteScope templates are stored as binary data. This is different from the text-based monitor sets used in earlier versions of SiteScope. Any changes to templates must be performed using the SiteScope interface.</li> <li>▶ Before exporting a template, all preferences including schedules, alerts, search/filter tags, credentials, and so forth, must be set to the default value to ensure that the correct values are used on the target SiteScope where it is imported.</li> </ul>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Understanding Templates” on page 1561</li> <li>▶ “Template Tree” on page 84</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>File Name</b>	Enter a name that is descriptive of the template or templates to be exported.
<b>Path</b>	<p>The location to which the template file is saved for export. Accept the default location, or enter a different location.</p> <p><b>Default value:</b> &lt;SiteScope_install_path&gt;\SiteScope\export</p>
<b>Template Tree</b>	<p>Select the templates you want to export.</p> <p><b>Default value:</b> All templates within the template container are exported.</p>



## Import Template Dialog Box

<b>Description</b>	<p>Enables you to import template configurations from other SiteScope installations. This allows you to efficiently replicate standardized monitor configurations across the enterprise.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click the template container into which you want to import the template or templates, and select <b>Import</b>.</p>
<b>Included in Tasks</b>	“Export and Import a Template” on page 1602
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Understanding Templates” on page 1561</li> <li>➤ “Template Tree” on page 84</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>File Name</b>	Enter the name of the file you want to import.
<b>Path</b>	<p>The location of the template file to be imported. Accept the default location, or enter a different location. The file must be on the SiteScope server or in a location that is accessible to the SiteScope server.</p> <p><b>Default value:</b> &lt;SiteScope_install_path&gt;\export</p>

## Publish Template Changes Wizard - Select Deployed Groups Page

<b>Description</b>	<p>The first page in the Publish Template Changes wizard. Use the Publish Template Changes wizard to check deployed groups for template compliancy and to update SiteScope objects deployed by templates whenever the source template is updated.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click a template, and select <b>Publish Changes</b>.</p> <p>Use the Select Deployed Groups Page to select groups associated with the source template for which you want to apply template changes.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ You can run the Publish Template Changes Wizard provided you have <b>Edit groups</b> permissions, and only on groups for which you have permissions in the <b>Allowed groups</b> list. Any deployed groups that are not in your allowed groups list are not displayed in the wizard.</li> <li>▶ The wizard opens only if there are deployments associated with the selected template. For details on deploying templates, see “Deploy the Template” on page 1585.</li> </ul>
<b>Included in Tasks</b>	“Publish Template Updates to Related Group Deployments” on page 1596
<b>Wizard Map</b>	<p>The Publish Template Changes wizard contains:</p> <p><b>Publish Template Changes Wizard - Select Deployed Groups Page</b> &gt; Review Compliancy Page &gt; Content Changes Dialog Box &gt; Modify Variables Page &gt; Publish Results Summary Page &gt; (Publish Template Changes Summary Report)</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Updating Template Deployments” on page 1578</li> <li>▶ “Template Tree” on page 84</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<List of groups associated with the selected template>	Select the groups associated with the selected template that you want to update with the template changes. <b>Default value:</b> All associated groups and subgroups are selected.
Enable delete on update	Select this option to ensure template compliancy. If selected, enables you to delete all SiteScope objects that are not in the source template from the deployed groups. <b>Default value:</b> Not selected
Verify template changes with remote servers	Select this option to verify the correctness of the monitor configuration changes in the selected template with the remote servers on which the template is deployed. <b>Note:</b> Selecting this option slows update performance time due to the remote connection. <b>Default value:</b> Not selected

### Review Compliancy Page

<b>Description</b>	Displays the structural differences between the source template and the deployed groups, and provides links to content differences in the deployed group objects.
<b>Included in Tasks</b>	“Publish Template Updates to Related Group Deployments” on page 1596
<b>Wizard Map</b>	The Publish Template Changes wizard contains: Publish Template Changes Wizard - Select Deployed Groups Page > <b>Review Compliancy Page</b> > (Content Changes Dialog Box) > Modify Variables Page > Publish Results Summary Page > (Publish Template Changes Summary Report)
<b>Useful Links</b>	“Updating Template Deployments” on page 1578

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<N> <b>deployed groups with structural/content differences</b>	Displays the deployed groups and group objects (subgroups, monitors, alerts, and remote servers) that have structural or content differences to the source template.
<N> <b>deployed groups with no structural/content differences</b>	Displays the deployed groups that have no structural or content differences to the source template. Groups with no deployment differences are displayed collapsed.
<b>Group Name</b>	<p>Displays the name of the deployed group and all its objects—subgroups, monitors, alerts, alert actions, and remote servers. Structural differences in the objects are displayed in the group tree hierarchy with the following text and color coding:</p> <ul style="list-style-type: none"> <li>➤ <b>Added.</b> Indicates a new object to be added to the deployed group. The object is displayed in green.</li> <li>➤ <b>Does not exist in template</b> (available only when the <b>Enable delete on update</b> option is not selected in the Select Groups page). Indicates an object that does not exist in the source template. The object is displayed in blue.</li> <li>➤ <b>Removed</b> (available only when the <b>Enable delete on update</b> option is selected in the Select Groups page). Indicates an object to be deleted from the deployed group. The object is displayed in red.</li> <li>➤ <b>Unused.</b> Indicates that the template remote server is not being used. An unused remote server is displayed in gray.</li> </ul>

GUI Element	Description
<b>Content Differences</b>	<p>Click the <b>View Differences</b> link to open the Content Changes dialog box and view differences in the property level for the deployed group or object. This link is displayed only for objects that contain content differences in properties, thresholds, and any other non-structural differences. For details on the user interface, see “Content Changes Dialog Box” on page 1629.</p> <p>Template remote servers that have been deployed are displayed in the <b>Microsoft Windows Remote Servers</b> or <b>UNIX Remote Servers</b> section. If a remote server already exists in Microsoft Windows/UNIX Remote Servers, it is not deployed again when the template is deployed.</p>

### **Content Changes Dialog Box**

<b>Description</b>	Use the Content Changes dialog box to view a list of all properties of the selected object to be updated, the current and the replacement values, and the property action status.
<b>Included in Tasks</b>	“Publish Template Updates to Related Group Deployments” on page 1596
<b>Wizard Map</b>	<p>The Publish Template Changes wizard contains:</p> <p>Publish Template Changes Wizard - Select Deployed Groups Page &gt; Review Compliancy Page &gt; (<b>Content Changes Dialog Box</b>) &gt; Modify Variables Page &gt; Publish Results Summary Page &gt; (Publish Template Changes Summary Report)</p>
<b>Useful Links</b>	“Updating Template Deployments” on page 1578

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Type</b>	The selected object type (Group, Monitor, Alert, Alert Action, Remote).
<b>Name</b>	The name of the selected object.
<b>Property Name</b>	The name of the property affected by publishing the change.
<b>Current Value</b>	The existing property value in the deployed group. This value is empty if the property is going to be added to the deployed group. <b>Note:</b> Existing password properties are displayed encrypted.
<b>Replacement Value</b>	The property value in the template. This value is empty if the property is going to be deleted from the deployed group. <b>Note:</b> <ul style="list-style-type: none"> <li>➤ Replacement password properties are displayed encrypted.</li> <li>➤ If you make changes to the <b>Depends on</b> property in a template monitor, the full path of the template monitor to which there is a dependence is displayed (for example, SiteScope\etc\template\group\CPU).</li> </ul>
<b>Action</b>	The status of the action ( <b>Modified, Added, Deleted, Ignored</b> ). Ignored status is used for baseline monitors, if there are no changes to the baseline thresholds.

 **Modify Variables Page**

<b>Description</b>	Use the Modify Variables page to add values for new variables in the deployed group. You can also edit existing variable values.
<b>Included in Tasks</b>	“Publish Template Updates to Related Group Deployments” on page 1596
<b>Wizard Map</b>	The Publish Template Changes wizard contains: Publish Template Changes Wizard - Select Deployed Groups Page > Review Compliancy Page > (Content Changes Dialog Box) > <b>Modify Variables Page</b> > Publish Results Summary Page > (Publish Template Changes Summary Report)
<b>Useful Links</b>	“Updating Template Deployments” on page 1578


The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Variable Name</b>	The name of a new or existing variable in the deployed group. A red asterisk indicates that the variable value is mandatory. <b>Note:</b> You can expand groups with variable values already filled, and modify the variables as required. You cannot expand groups that do not contain variables.
<b>Variable Value</b>	Enter a value for new variables added to the deployed group. You can also edit existing variable values. <b>Note:</b> <ul style="list-style-type: none"> <li>▶ The variable value for the remote server is read only and cannot be changed.</li> <li>▶ Hypertext tags in a variable string cause the string to be truncated and be incorrectly displayed in the Variable Value box (part of the string is displayed in the text label).</li> </ul>

 **Publish Results Summary Page**

<b>Description</b>	Displays a summary of the published template updates.
<b>Included in Tasks</b>	“Publish Template Updates to Related Group Deployments” on page 1596
<b>Wizard Map</b>	The Publish Template Changes wizard contains: Publish Template Changes Wizard - Select Deployed Groups Page > Review Compliancy Page > (Content Changes Dialog Box) > Modify Variables Page > <b>Publish Results Summary Page</b> > (Publish Template Changes Summary Report)
<b>Useful Links</b>	“Updating Template Deployments” on page 1578

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
	Click to export the results of publishing for each root group to a PDF file. For details, see “Publish Template Changes Summary Report” on page 1633.
<b>Group Name</b>	Displays the root group name and the group’s objects (subgroups and monitors).
<b>Reason</b>	If SiteScope is unable to publish changes to a deployed group, the reason for failure is displayed for each monitor in the group.



## Publish Template Changes Summary Report

The following is an example of the Publish Template Changes Summary Report.

Publish Template Changes Summary Report				
Total number of deployed groups for publishing changes: 1				
Total number of deployed groups that were not updated: 0				
Total number of deployed groups that were successfully updated: 1				
Successfully Changed Deployed Groups				
Deployed Root Group: SiteScope\Examples\System monitors subgroup\docs\Windows monitors for R205				
Type	Name	Reason	Message	
Monitor	SiteScope\Examples\System monitors subgroup\docs\Windows monitors for R205\Cpu monitor on R205	Successfully modified		
	Property Name	Deployment Value (previous)	Template Value (current)	Action on Property Value
	Server	SiteScope Server	%%host%% remote windows	Successfully modified
Monitor	SiteScope\Examples\System monitors subgroup\docs\Windows monitors for R205\Cpu monitor on R205	Successfully modified		
	Property Name	Deployment Value (previous)	Template Value (current)	Action on Property Value
	Server	SiteScope Server	%%host%% remote windows	Successfully modified
Remote Server	%%host%% remote windows	Successfully added		

<b>Description</b>	Displays information about the template changes published to the deployed groups. It also displays information for group objects that failed to update. Results are at the object level (Group, Monitor, Alert, Alert Action, Remote Server).
<b>Included in Tasks</b>	“Publish Template Updates to Related Group Deployments” on page 1596

<b>Wizard Map</b>	The Publish Template Changes wizard contains: Publish Template Changes Wizard - Select Deployed Groups Page > Review Compliancy Page > (Content Changes Dialog Box) > Modify Variables Page > Publish Results Summary Page > ( <b>Publish Template Changes Summary Report</b> )
<b>Important Information</b>	The Publish Template Changes Summary Report PDF is not supported in Firefox 2.x.
<b>Useful Links</b>	“Updating Template Deployments” on page 1578

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):




GUI Element	Description
<Report summary>	The report summary shows the total number of root groups selected for publishing changes, including the number of groups that were successfully and unsuccessfully changed.
<b>Deployed Root Group</b> <group path>	The name of the deployed group and all group objects that were successfully or unsuccessfully updated with the template changes. The deployed groups that were not updated are displayed first.  <b>Note:</b> For changes to be published, all changes in the root group hierarchy must succeed. If any changes to a group object fail, all changes to that group are rolled back.
<b>Type</b>	The object type (Group, Monitor, Alert, Alert Action, Remote Server).
<b>Name</b>	The name of the object and its path.
<b>Reason</b>	The publish status for the object (Successfully added, Successfully modified, Successfully deleted, Failed to add, Failed to modify, Failed to delete, Unchanged).

GUI Element	Description
<b>Message</b>	For deployed group objects that were not updated by the template changes, the reason for the failure to publish the changes.
<Property details>	<p>For deployed group objects that had content changes:</p> <ul style="list-style-type: none"> <li>▶ <b>Property Name.</b> The name of the property that was updated.</li> <li>▶ <b>Deployment Value (previous).</b> The previous property value in the deployed group. This value is empty for a property that was added to the deployed group. Previous password variables are displayed encrypted.</li> <li>▶ <b>Template Value (current).</b> The replacement property value in the deployed group. This is the current property value in the template. This value is empty if the property was deleted from the deployed group. Replacement password variables are displayed decrypted.</li> <li>▶ <b>Action on Property Value.</b> The type of change made to the property value (Successfully modified, Successfully added, Successfully deleted).</li> </ul>

## Select Group Dialog Box

<b>Description</b>	<p>Enables you to select a group in the monitor tree to which you can deploy templates. Alternatively, you can select the SiteScope node, and create a new group to which you can deploy templates.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click the template you want to deploy, and select <b>Deploy Template</b> or <b>Deploy Template Using CSV</b>.</p>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</li> <li>▶ “Publish Template Updates to Related Group Deployments” on page 1596</li> <li>▶ “Deploy a SiteScope Solution Template – Workflow” on page 1669</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Updating Template Deployments” on page 1578</li> <li>▶ “SiteScope Solution Templates” on page 1665</li> <li>▶ “Template Tree” on page 84</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
 SiteScope	Represents the SiteScope root group. You can deploy the templates in the SiteScope root group, or click the <b>New Group</b> button and create a new group to which you can deploy the templates.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors). Select the group to which you want to deploy the templates, or click the <b>New Group</b> button and create a new group in which you can deploy the templates.
	Represents the collection of available health monitors that are deployed to check proper functioning of SiteScope monitors.

## Deployment Values Dialog Box

<p><b>Description</b></p>	<p>Enables you to enter variable values when deploying the template.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click the template that you want to deploy (it must contain variables), and select <b>Deploy Template</b>. In the Deploy Template dialog box, select the group in which you want to deploy the template. The Deployment Values dialog box opens.</p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ To deploy monitors to multiple servers at the same time, enter the server names or addresses separated by a comma (","). When doing this, the value in the <b>Host</b> property for the template remote server referenced by the monitors must consist of a variable value, and only one variable is allowed.</li> <li>▶ You can deploy a template, regardless of its content, provided you have edit permissions on the deployment target group. You do not require edit permissions on the template objects such as monitors, remotes, and alerts.</li> <li>▶ An error message is displayed if a monitor cannot be deployed. This may occur, for example, when deploying the Disk Space monitor template, if the disk drive does not exist on the deployed server.</li> </ul>
<p><b>Included in Tasks</b></p>	<ul style="list-style-type: none"> <li>▶ “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</li> <li>▶ “Deploy a Template Using the User Interface” on page 1590</li> <li>▶ “Publish Template Updates to Related Group Deployments” on page 1596</li> <li>▶ “Template Tree” on page 84</li> </ul>
<p><b>Useful Links</b></p>	<p>“Updating Template Deployments” on page 1578</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<variable name>	Each variable that is referenced in a template object prompts the display of a corresponding entry box when the template is deployed. The variable name is used as a label for the text entry box. Enter deployment values for the variables.
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <SiteScope root directory>\logs\silent_deployment.log. <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected

## Select CSV File Box Dialog Box

<b>Description</b>	<p>Enables you to select the CSV file to use when deploying a template.</p> <p><b>To access:</b> Use one of the following:</p> <ul style="list-style-type: none"> <li>➤ Open the <b>Templates</b> context. In the template tree, right-click the template you want to deploy, and select <b>Deploy Template Using CSV</b>. In the Select Group dialog box, select the group to which you can deploy the template, and click <b>OK</b>.</li> <li>➤ Open the <b>Monitors</b> context. In the monitor tree, right-click the group to which you want to deploy the template, and select <b>Deploy Template Using CSV</b>. In the Select Template dialog box, select the template that you want to deploy, and click <b>OK</b>.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>➤ “Configure a SiteScope Monitoring Solution Using a Template – Workflow” on page 1580</li> <li>➤ “Deploy a Template Using a CSV File” on page 1592</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Updating Template Deployments” on page 1578</li> <li>➤ “Template Tree” on page 84</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>CSV file</b>	<p>The CSV file to use for deploying the variable values defined in the template. Click the <b>Select</b> button, and select a CSV file to use for the template deployment.</p> <p><b>Note:</b> You can only use a file with a CVS extension.</p>
<b>Verify monitor properties with remote server</b>	<p>Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>

 **Generate Auto Deployment XML**

<b>Description</b>	<p>Enables you to create an XML file to use for automatically deploying the templates in the highlighted template container. After you generate the XML file, you can edit the file and use it to deploy the templates from the file directory not in the SiteScope user interface.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, right-click the template container for which you want to create an auto deploy XML file, and select <b>Generate XML</b>.</p>
<b>Included in Tasks</b>	“Deploy a Monitoring Structure Using an XML File” on page 1653
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Auto Template Deployment Overview” on page 1644</li> <li>▶ “Template Tree” on page 84</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>File Name</b>	Enter the name of the XML file to create. This is the file you can edit and use to automatically deploy the templates in this template container.



GUI Element	Description
<p><b>Path</b></p>	<p>The location in which the XML file is saved. Accept the default location, or enter a different location.</p> <p><b>Default value:</b>                      &lt;SiteScope_install_path&gt;\SiteScope\persistence\autodeployment\drafts</p> <p><b>Note:</b> If an XML file has been generated previously using the same <b>File Name</b> and <b>Path</b>, the previously saved XML file is not overwritten. The previous file is renamed with the following addition: <b>_bck&lt;number of backup&gt;</b>. For example, if you enter CPUtemplate as the <b>File Name</b> and accept the default location, the existing file in the default folder becomes CPUtemplate.xml_bck1 and the current XML file being generated is saved as CPUtemplate.xml.</p>
<p><b>Template Tree</b></p>	<p>Select the templates for which to create the XML file. The XML file's contents are based on the objects in the template you select. For each template selected, the generated XML includes a separate deploy section.</p>



## Auto Template Deployment

This chapter includes the main concepts, tasks, and reference information for SiteScope auto template deployment.

### **This chapter includes:**

#### **Concepts**

- ▶ Auto Template Deployment Overview on page 1644
- ▶ Creating and Working with the XML File on page 1645
- ▶ XML File Example and Variables on page 1646
- ▶ XML Validator on page 1650
- ▶ Publishing Template Changes Using the XML on page 1650
- ▶ Deployment Results on page 1653

#### **Tasks**

- ▶ Deploy a Monitoring Structure Using an XML File on page 1653
- ▶ Encrypt Text on page 1657
- ▶ Update a Deployment on page 1658

#### **Reference**

- ▶ XML Tag Reference on page 1660

**Troubleshooting and Limitations** on page 1663

## Auto Template Deployment Overview

SiteScope enables you to automatically deploy a SiteScope template or solution template using an XML file external to the SiteScope user interface. The XML file is used to deploy the objects defined in the template, which must include a parent group and can include subgroups, monitors, a remote server, alerts, and variable definitions. You can edit the XML file to assign variable definitions for mandatory, global, and instance variables.

For details on creating templates, see “SiteScope Templates Overview” on page 1558. For details on working with solution templates, see “Solution Templates Overview” on page 1665.

You can also use the auto template deployment to publish template changes to deployed groups. The auto template deployment uses the same functionality as the Publish Template Changes Wizard. For details on how the wizard works, see “Updating Template Deployments” on page 1578.

Auto template deployment is an alternative to using the user interface to deploy templates and publish template changes to deployed groups. It is better suited than the user interface for working with scripts and deploying onto multiple SiteScopes. This is because it uses standard XML scripting and can be deployed onto multiple SiteScopes using one file.

## Creating and Working with the XML File

Use one of the following options to create the XML file:

- ▶ Generate and edit your XML in any tool that supports text. The file must be based on the XSD file supplied in the SiteScope file directory. The XSD file is a basic XML file which already includes the appropriate tags, elements, and attributes for creating your own version of the deployment XML.
- ▶ Generate the deployment XML file using the SiteScope interface from a template container or solution template. Each template container and solution template includes the option to generate this auto template deployment XML file. For details, see “Generate Auto Deployment XML” on page 1640.

The XML you use, whether generated from the template or solution template, or generated manually, must be a valid XML and match the ATD schema (XSD). You can use the dedicated tool to validate your XML file.

Deploying the XML file is dependent on the target SiteScope having the relevant template or solution template in its monitor tree. You deploy the template or solution template by copying the XML file into the persistency folder of the target SiteScope with the relevant template or solution template. You can group several deployments into a single XML file.

## XML File Example and Variables

For a reference detailing all the XML tags, elements, and attributes included in the auto template deployment file, see “XML Tag Reference” on page 1660.

Each auto template deployment XML must begin with the following declarations:

- ▶ `<?xml version="1.0" encoding="UTF-8" ?>` This states that this is an XML with UTF-8 character encoding.
- ▶ `<sitescope:sitescopeRoot ...>` This is the schema declaration. Despite the URLs mentioned, this does not try to connect to any location outside of your SiteScope at any time.

Each section of the XML file begins with one of the following tags, with the instruction to perform one of the following actions:

- ▶ `<sitescope:templateDeployment>` Deploys a template or solution template. You can have multiple instances within the same XML file.
- ▶ `<sitescope:templateDeployUpdate>` Publishes changes to an existing deployment.

Within each action, you must specify the following:

- ▶ `<deploy:fullPathToTemplate>` The path to the template within the SiteScope tree in the user interface, not including the SiteScope root node. In the XML file example, this value is `Templates/Windows`.
- ▶ `<deploy:fullPathToDestinationGroup>` The path, within the SiteScope tree, of the target group upon which the action is performed. For example, in the XML file example, any template group objects are created as subgroups within the following group `SiteScope/Windows_Monitors`.

This section contains the following topics:

- ▶ “XML File Example” on page 1647
- ▶ “Variables” on page 1648

## XML File Example

Here is an example of the auto template deployment XML file. This file was generated from the user interface.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--SiteScope deployment descriptor-->
<sitescope:sitescopeRoot xmlns:sitescope="./sitescope" xmlns:deploy="./deploy"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="./sitescope
../schemas/sitescope.xsd ">
  <!--To deploy use "templateDeployment", to update an existing deployment use
templateDeploymentUpdate (this element can have the attribute enableDeleteOnUpdate with values of
yes/no)-->
  <sitescope:templateDeployment>
    <!--Path to source template in SiteScope tree (not including the root node)-->
    <deploy:fullPathToTemplate>Templates/Windows</deploy:fullPathToTemplate>
    <!--Path to destination group in SiteScope tree (not including the root node). New group
will be created if need be-->
    <deploy:fullPathToDestinationGroup>
SiteScope/Windows_Monitors</deploy:fullPathToDestinationGroup>
    <!--Mandatory variables names-->
    <deploy:mandatoryFields>group frequency</deploy:mandatoryFields>
    <!--Global values for variables in current template-->
    <deploy:globalVariables>
      <deploy:variables encrypted="yes" name="password" value="(sisp)d5JLOSwaVfE="/>
      <deploy:variables encrypted="no" name="user" value="admin"/>
      <deploy:variables encrypted="no" name="frequency" value="600"/>
    </deploy:globalVariables>
    <!--Add here local variables for a deploy instance (overrides global variables with same
name)-->
    <deploy:templateInstanceDeployVariable>
    <deploy:variables encrypted="no" name="group" value="Critical_monitors"/>
    <deploy:variables encrypted="no" name="frequency" value="600"/>
    </deploy:templateInstanceDeployVariable>
    <deploy:templateInstanceDeployVariable>
    <deploy:variables encrypted="no" name="group" value="Minor_monitors"/>
    <deploy:variables encrypted="no" name="frequency" value="6000"/>
    </deploy:templateInstanceDeployVariable>
  </sitescope:templateDeployment>
</sitescope:sitescopeRoot>
```

## Variables

Once the template and destination have been specified, the next section of the XML file deals with the template variables and values. The XML file gives you the flexibility of defining variables and their values, declaring mandatory variables, and determining if their corresponding values should be applied globally across the deployment or per instance.

If you generated the XML file from the user interface and if a variable has a defined value, that value is assigned to the variable in the XML file.

### Mandatory Variables

A declaration of any mandatory variables in the template appears in the `<deploy:mandatoryFields>` tag. If a variable is declared mandatory, a corresponding value for the variable must be defined in the in the file.

If you generated the XML from the user interface and if the **Mandatory** option was selected when creating or editing a variable, that variable appears in the `<deploy:mandatoryFields>` tag. You can also manually add a variable name to this list to declare it mandatory.

In the file example above, group and frequency have been defined as mandatory variables. Values for these variables must appear within the `<deploy:variables>` tags for either the `<deploy:globalVariables>` or the `<deploy:templateInstanceDeployVariables>`.

### Global Versus Instance Variables

The optional `<deploy:globalVariables>` tag includes the default global template variables for the deployment. Defining global template variables is optional. When you define a global template variable, you can overwrite the variable's value by identifying a different variable value in the deployment instance area of the file (`<templateInstanceDeployVariables>` tag). Global variable values can be overwritten with a different value in each deployment instance.



Multiple instances of a template that are deployed into the same location onto the same SiteScope, as seen in the XML file example, must include a variable for the group name. Group name must be made a mandatory variable and given a different value in each deployment instance. The group template object must have the same variable defined as its value. The template could include other groups whose name value is not a variable and those groups would be deployed once.

In the XML file example above, there are two instances of the deployment, so a variable called `group` has been defined as mandatory and a different value has been given to it in each instance deployment (`Critical_monitors` and `Minor_monitors`). This results in two groups created under the group object of the template with the same monitor objects.

The following groups would result from the XML file example being deployed:

- ▶ `SiteScope/Windows_Monitors/Critical_monitors` in the first instance of the deployment.
  - ▶ Included in this group would be any monitors and alerts defined in the template. Any of the template monitor objects whose frequency value was defined as the variable `frequency` would have a value of 600 or every 10 minutes.
- ▶ `SiteScope/Windows_Monitors/Minor_monitors` in the second instance of the deployment.
  - ▶ Included in this group would be any monitors and alerts defined in the template. Any of the template monitor objects whose frequency value was defined as the variable `frequency` would have a value of 6000 or every hour.

---

**Note:** If you have any system variables defined in a template (those defined by `$$` and not `%%`), they are treated as normal variables in the auto template deployment XML file. The same limitations that apply to using system variables in templates apply to using them in the XML file.

---

## XML Validator

The XML validator is a utility that validates the XML file against the schemas used by the auto template deployment. It does not validate the SiteScope deployment itself. The path to the validator file is:

- ▶ For Windows: `<SiteScope root directory>/tools/AutoDeployment/validate_template_xml.bat`
- ▶ For UNIX: `<SiteScope root directory>/tools/AutoDeployment/validate_template_xml.sh`

This utility checks the structure of the XML against the XSD files to make sure that the contents of the file are valid XML and correspond to the XSD. It also validates that there have been values defined for all mandatory variables. The values can be defined either as global variables or deployment instance variables. If the validation fails, the reason for the failure is printed to screen.

## Publishing Template Changes Using the XML

You can also use the auto template deployment XML to publish template changes to update the values or structure of a deployed group. If the group's **Source Template** field is identified as the same template that the XML is referencing, you can update the values and objects of the group using the auto template deployment XML.

The XML uses the same functionality as the Publish Template Changes Wizard but without having to access the user interface. In the XML file, you can identify values for variables to use for publishing the changes in the template. For details on the wizard and the template update feature, see “Updating Template Deployments” on page 1578.

You can use auto template deployment to publish the changes made to a template onto the template's deployed groups in the same way you use the XML to create a group deployment. Once the template has been modified, you create the XML and copy/paste the edited XML into the persistency folder of the target SiteScope machines.

This section includes the following topics:

- “Update Deployment XML Tag Details” on page 1651
- “Template Update Report” on page 1652

## Update Deployment XML Tag Details

The XML file for updating the values or objects of a deployed group must use the `<siteScope:templateDeploymentUpdate>` tag (and not the `<siteScope:templateDeployment>` tag used for deploying the template). For details on the elements and attributes to use in the XML file, see “XML Tag Reference” on page 1660.

Within the `<siteScope:templateDeploymentUpdate>` tag, you can select to give the `enableDeleteOnUpdate` attribute a value of **yes** to make sure that any objects within the deployed groups that do not appear in the template referenced by the auto template deployment XML are deleted when updating the deployment with the XML file. Enter a value of **no** to make sure that all objects within the group are retained, even if they do not appear in the template referenced by the XML file, after the updating the deployment. For details on this option in the Publish Template Changes Wizard, see “Enable delete on update” on page 1627.

To successfully perform the update, you must define the target SiteScope group name of the deployed group as the value of the `deploy:fullPathToDestinationGroup` tag. The `fullPathToDestination` must end with the root group of the deployment, the equivalent of the template's root group. Each deployment section updates one group so if you have multiple groups, you must define separate deployment update sections for each and define the group name for each.

## Template Update Report

After performing the auto template deployment update, a report is available in XML format. The report file is named with the name of the XML file along with a time stamp and the string **\_reports**. These reports are available in the following location: **<SiteScope root directory>\persistence\autodeployment\reports**.

The report is in XML format and includes the following tags at the beginning:

- ▶ **totalNumberOfDeployments**
- ▶ **totalNumberOfFailedDeployments**
- ▶ **totalNumberOfSuccessDeployments**

The **<publishChangesSummaryPage>** section of the XML appears for each deployment instance listing the details of what has been updated. Unsuccessfully changed deployments are specified first in the file.

This file is an XML version of the PDF file created by the Publish Template Changes Wizard if using the SiteScope user interface to update deployed groups. For details on the report, see “Publish Template Changes Summary Report” on page 1633.

## Deployment Results

When you copy the XML file, for both deploying and updating, into the persistency folder of the target SiteScope, the file is copied into one of two directories as follows:

- **<SiteScope root directory>\persistency\autodeployment\successHistory** directory includes those XML files that deployed or updated successfully all instances of the deployed group.
- **<SiteScope root directory>\persistency\autodeployment\failHistory** directory includes those XML files that failed to deploy or update any instance of the deployed group. If even one instance failed and all the others succeeded, the XML is published to this folder.

The XML file name is changed to include an underscore and a timestamp added to the original name of the XML file. For example the XML file named CPUgroups.XML that succeeded in deploying all its groups and instances is saved to the **<SiteScope root directory>\persistency\autodeployment\successHistory** directory and is now named CPUgroups\_1203951216931.xml.

## Deploy a Monitoring Structure Using an XML File

This task describes how to perform an auto template deployment. You can follow the same steps for deploying a Solution Template.

This task includes the following steps:

- “Prerequisites” on page 1654
- “Create the XML File” on page 1654
- “Edit the XML File” on page 1655
- “Encrypt Fields Such as Passwords (Optional Step)” on page 1655
- “Validate the XML File” on page 1655
- “Copy the Validated XML to the SiteScope Server Machines” on page 1656
- “Check If Deployment Was Successful” on page 1656

## 1 Prerequisites

Each SiteScope into which you want to automatically deploy a template must include the template within a template container. The template must have a group object at the top level. All other objects must be created within that group. The template can contain subgroups, monitors, alerts, one remote server, and variables.

If you are working with multiple SiteScopes:

- ▶ You can create the template in one SiteScope and export it to other SiteScopes using the Export/Import options in the Template containers context menu. For details on how to do this, see “Export Template Dialog Box” on page 1623 and “Import Template Dialog Box” on page 1625.
- ▶ If you are working in HP Business Availability Center, you can copy templates from one SiteScope to another using the Sync SiteScope Wizard in System Availability Management Admin. For details on the wizard interface, see “Sync SiteScopes Wizard - Select Source and Targets Page” on page 139.

## 2 Create the XML File

You can create the XML file using one of these options:

- ▶ Right-click the template container and select **Generate XML File** in the context menu. When deploying solution templates, this option appears at the template level. For details on this user interface option, see “Generate Auto Deployment XML” on page 1640.
- ▶ Create the XML file using a dedicated XML application. The file must be a valid XML file and based on the XSD files located in the following directories:
  - ▶ **<SiteScope root directory>/conf/xsds/deploy.xsd**
  - ▶ **<SiteScope root directory>/conf/xsds/sitescope.xsd**

### 3 Edit the XML File

You must edit the XML file to enter the values necessary for deployment. For details on editing the file and a sample of the file, see “XML File Example and Variables” on page 1646.

For details on the XML file’s tags, see “XML Tag Reference” on page 1660.

---

**Note:** If the XML is generated from the user interface, mandatory variable fields are generated based on the templates mandatory variables. If you create the XML file, and there are fields that are mandatory for successful deployment, you must make sure that these fields have been assigned values before deploying the XML.

---

### 4 Encrypt Fields Such as Passwords (Optional Step)

For deploying templates that include fields that you do not want to appear in viewable text, use the encryption tool and follow the steps in the procedure for encrypting text. For details on how to perform this task, see “Encrypt Text” on page 1657.

### 5 Validate the XML File

We recommend that you validate the XML file before it is deployed.

Use the validation tools located in the following directories:

- For Windows: `<SiteScope root directory>/tools/AutoDeployment/validate_template_xml.bat`
- For UNIX: `<SiteScope root directory>/tools/AutoDeployment/validate_template_xml.sh`

For details on this topic, see “XML Validator” on page 1650.

## 6 Copy the Validated XML to the SiteScope Server Machines

Copy the XML file into the `\persistence\autodeployment` directory on each SiteScope machine where you want to deploy the templates in the XML.

The templates are automatically deployed every two minutes by default. You can change the frequency in Infrastructure Setting Preferences in the following field: **Auto Deployment Check Frequency** (Property name: `_autoDeploymentCheckFrequency`).

---

**Note:** If the XML file does not pass validation when attempting to deploy, the deployment fails. We recommend that you validate the XML file before copying onto the persistence directories of the SiteScope server machines.

---

## 7 Check If Deployment Was Successful

You can check if the deployment was successful by searching in the target SiteScope's `<SiteScope root directory>\persistence\autodeployment` directory to see if the XML was copied into the `successHistory` subdirectory or the `failHistory` subdirectory.

For details on this topic, see “Deployment Results” on page 1653.

You can also check the SiteScope's Error Log.



## Encrypt Text

This task describes how to encrypt text for a field that should not appear in viewable text, for example a password. This tool encrypts the field only in the XML; the templates themselves control the encryption of variables in the persistency directory.

### To encrypt text for use in the deployment XML:

- 1 Run the following batch file:
  - ▶ For Windows: `<SiteScope root directory>/tools/AutoDeployment/encrypt_password.bat`
  - ▶ For UNIX: `<SiteScope root directory>/tools/AutoDeployment/encrypt_password.sh`
- 2 Open a command prompt window.
  - ▶ In Windows, drag and drop the file into your command prompt window.
  - ▶ In UNIX, you must run the .sh file from its directory.
- 3 Enter space and the password value (for example Mypassword). Click ENTER.
- 4 Use the returned string as a value for the encrypted variable in the XML file. You must change the value of the attribute **encrypted** to **yes** and the **value** of the variable attribute to the returned string.

For example, the following value was generated by the encryption tool:

```
<deploy:variables encrypted="yes" name="password" value="(sisp)d5JLOSwaVfE="/>
```

## Update a Deployment

This task describes how to use the auto template deployment XML to update an existing, deployed group. You can update the structure of the deployment if the template was changed or update object properties by giving new values to the variables that are declared in the template for those properties.

The task follows the same steps as the task to deploy a template with the exceptions and additional information listed in the steps here. For details on the deployment task, see “Deploy a Monitoring Structure Using an XML File” on page 1653.

This task includes the following steps:

- “Prerequisites” on page 1658
- “Create and Edit the XML File to Update Objects and Values” on page 1659
- “Copy the Publish Template Update XML to the Target SiteScopes” on page 1659
- “Encrypt Text Such as a Password (Optional Step)” on page 1659
- “Validate the Publish Template Update XML” on page 1659
- “Results Report” on page 1659

### 1 Prerequisites

The **Source Template** field of the deployed groups that you want to update must be identical to the template in the XML deployment update file. This is in addition to the updated template existing in the target SiteScope.

## 2 Create and Edit the XML File to Update Objects and Values

When working with the XML file, you must do the following:

- Use the `<templateDeploymentUpdate>` tag instead of the `<templateDeployment>` tag.
- Enter a **yes** or **no** value for the **enableDeleteOnUpdate** attribute of the `<templateDeploymentUpdate>` tag.
- Define the **deploy:fullPathToDestinationGroup** tag with the group name to be updated as the value for this tag.

For details on these tags and the update XML file, see “Update Deployment XML Tag Details” on page 1651.

## 3 Copy the Publish Template Update XML to the Target SiteScopes

Copy the publish template update XML to the target SiteScope’s **persistence** directory as you would when deploying the auto template deployment XML file.

## 4 Encrypt Text Such as a Password (Optional Step)

For details on performing this task, see “Encrypt Text” on page 1657.

## 5 Validate the Publish Template Update XML

Use the validator tool to validate the edited XML file as you would when deploying the auto template deployment XML file.

## 6 Results Report

After deploying the update auto template deployment XML, a results report file is created in XML format. These reports are available in the following location: `<SiteScope root directory>\persistence\autodeployment\reports`.

For details on the report, see “Template Update Report” on page 1652.

## XML Tag Reference

The following tables list all the elements and attributes used in the auto template deployment XML files:

- “Elements Table” on page 1660
- “Attributes Table” on page 1662

### Elements Table

Elements	Description
sitescope:sitescopeRoot	This must be the first tag in the XML file giving the instruction to create the deployment, the version of XML used, and the location of the XSD file. <b>Note:</b> This is the first element in all XML files related to SiteScope.
sitescope:template Deployment	This tag enables the deployment of the template or solution template, creating new group structures in the target SiteScope. This is the default tag used in the XML file when generated from the user interface.
sitescope:template DeploymentUpdate	This tag enables publishing the changes of a template that has been updated. These changes can be applied to the monitoring structure of a group whose <b>Source Template</b> field matches the template identified in the XML. The XML file also enables you to update the values of the variables used in the template.  For example, if you want to add alerts or an additional monitor to an existing group that was created by a template, you can modify the template and deploy it using this tag.
deploy:fullPathToTemplate	This tag gives the full path, within the SiteScope tree, of the template or solution template to be deployed.  <b>Syntax:</b> <template container name>/<template name>

Elements	Description
<p>deploy:fullPathToDestinationGroup</p>	<p>This tag gives the full path location within the SiteScope tree of the group name where the deployed monitoring structure is to be created. If this tag has no value, the deployment is created at the SiteScope node level.</p>
<p>deploy:mandatoryFields</p>	<p>The values within this tag are those variables that were selected as mandatory fields when the template was created. If there are any values appearing within this tag, they must be given a value in the <b>&lt;deploy:globalVariables&gt;</b> tag for global variables or the <b>&lt;deploy:variables&gt;</b> tag for other variables. If there are no corresponding values for these mandatory fields, the XML fails validation.</p>
<p>deploy:globalVariables</p>	<p>This tag marks the section of the file that includes the variables that are deployed across the entire selected template.</p> <p>Includes attributes. For details, see “Attributes Table” on page 1662.</p>
<p>deploy:templateInstanceDeployVariable</p>	<p>This tag marks the section of the file that includes the variables that are deployed per instance of the selected template.</p> <p>If the same variable appears in the <b>&lt;deploy:globalVariables&gt;</b>, the instance variable value overrides the global variable value only for the instance in which it appears. All other instances have the value entered in the <b>&lt;deploy:globalVariables&gt;</b> section.</p> <p>Includes attributes. For details, see “Attributes Table” on page 1662.</p>
<p>deploy:variables</p>	<p>This tag defines the variables and their values.</p> <p>Includes attributes. For details, see “Attributes Table” on page 1662.</p>

## Attributes Table

Parent Element	Attribute	Description
templateDeploymentUpdate	enableDeleteOnUpdate	<p>Indicates whether any instances of objects appearing in a deployment of a template should be deleted when not appearing in the XML file used for updating the structure of a deployment.</p> <p><b>Possible values:</b> yes, no</p> <p>For details on this option, see “Enable delete on update” on page 1627.</p>
deploy:globalVariables	encrypted	<p>Indicates whether the value of the variable’s field is encrypted or not.</p> <p><b>Possible values:</b> yes, no</p> <p>To encrypt a value, use the encryption tool to provide the value for the variable. For details, see “Encrypt Text” on page 1657.</p>
	name	The name of the variable.
	value	The value of the variable.
deploy:variables	encrypted	<p>Indicates whether the value of the variable’s field is encrypted or not.</p> <p><b>Possible values:</b> yes, no</p> <p>To encrypt a value, use the encryption tool to provide the value for the variable. For details, see “Encrypt Text” on page 1657.</p>
	name	The name of the variable.
	value	The value of the variable.

## Troubleshooting and Limitations

All notes, limitations, and troubleshooting issues that apply to SiteScope templates, solution templates, and the Publish Template Changes Wizard also apply to the functionality of the auto template deployment.

This section includes the following topics:

- ▶ “I18N Users” on page 1663
- ▶ “Solution Templates” on page 1663
- ▶ “Characters Not Permitted in XML” on page 1664
- ▶ “Unable to Auto Deploy Template with No Groups” on page 1664

### **I18N Users**

- ▶ Do not edit the XML file using Notepad. The file cannot be parsed because Notepad adds an extra character to the beginning of the file. This character is not visible but prevents the file from being parsed when not in English. Use Wordpad or an XML editor instead.
- ▶ If the path to the SiteScope root directory includes non-English characters, the validation tool cannot be used to validate the XML before it is copied to the SiteScope’s persistency directory. This means that there is no validation that the XML follows the XSD or that mandatory fields have values.

### **Solution Templates**

You cannot perform auto template deployment for the following Solution Templates because the variables in these solution templates are dynamically created and cannot be given a value in the XML file:

- ▶ JBoss Application Server 4.x
- ▶ WebLogic Application Server
- ▶ WebSphere 5.x Application Server
- ▶ WebSphere 6.x Application Server

## Characters Not Permitted in XML

Avoid using the ampersand (&), quote marks (“), and angle brackets (< >) characters, as they are not permitted in XML attribute values.

To escape illegal XML characters, use a common encoding, (for example, &amp; instead of &), or enclose the character with the CDATA (character data) section. For details, see [http://xmmssc-www.star.le.ac.uk/SAS/xmmsas\\_20070308\\_1802/doc/param/node24.html](http://xmmssc-www.star.le.ac.uk/SAS/xmmsas_20070308_1802/doc/param/node24.html).

## Unable to Auto Deploy Template with No Groups

If you attempt to automatically deploy a template where the template has no parent group defined (that is to say, the template has monitors directly under the root template), the deployment fails and the following error is written to the <SiteScope root directory\logs\>error.log file:

```
[Autodeployment new XML detection] (XMLAutomationParser.java:294) ERROR  
- Prerequisites of template structure are unmet. Template must be rooted by only  
one group.
```

Note that Auto deployment fails even if **Allow creation of template monitors directly under template** is selected in **Preferences > Infrastructure Preferences > Template Settings**.

**Workaround:** Deploy the template manually (by right-clicking the template in the Template tree, and selecting **Deploy Template**).



# 133

---

## SiteScope Solution Templates

This chapter includes the main concepts, tasks, and reference information for SiteScope solution templates.

### **This chapter includes:**

#### Concepts

- ▶ Solution Templates Overview on page 1665

#### Tasks

- ▶ Deploy a SiteScope Solution Template – Workflow on page 1669

#### Reference

- ▶ Solution Template User Interface on page 1671
- ▶ Troubleshooting and Limitations on page 1672

### **Solution Templates Overview**

SiteScope solution templates are preconfigured monitor set templates designed to monitor popular enterprise applications and network systems. Using solution templates, you can rapidly deploy a combination of standard SiteScope monitor types and solution-specific monitors with settings that are optimized for monitoring the availability, performance, and health of the target application or system. For example, the solutions for Microsoft Exchange monitoring include performance counter, event log, and Exchange application specific monitor types.

Deploying the solution creates a new monitor group container in which the individual solution monitors are added. You can deploy a solution template for each server in your environment. For solution templates that use the system variable `SERVER_LIST`, you can deploy the solution on multiple remote hosts.

This section also includes:

- “List of Solution Templates” on page 1666
- “Customizing Solution Templates” on page 1668
- “Notes and Limitations” on page 1668

## List of Solution Templates

The following table lists solution templates available for SiteScope. For more information about each solution and the solution specific monitor types, see the chapter for the specific solution template.

Solution Name	Description
Active Directory Solution Template	Monitors the performance and efficiency of Microsoft domain controllers.
AIX Host Solution Templates	Monitors performance, availability, and health for AIX host machines.
HP Quality Center Solution Templates	Monitors performance, availability, and health for HP Quality Center 9.x and 10.x application servers on Windows and UNIX, HP Quality Center license usage and expiration time on an Oracle Database server, and HP QuickTest Professional license server application and system availability.
HP Service Manager Solution Template	Monitors HP Service Manager application servers availability and system status on Windows and UNIX platforms.
JBoss Application Server Solution Template	Monitors performance, availability, and health for JBoss environments.
Linux Host Solution Templates	Monitors performance, availability, and health for Linux host machines.

Solution Name	Description
Microsoft Exchange Solution Templates	Includes individual solution options for monitoring application health, message flow, and usage statistics for Microsoft Exchange 5.5, 2000, 2003, and 2007 servers.
Microsoft IIS Solution Template	Monitors performance, availability, and health for IIS 6.0 environments.
Microsoft SQL Server 2005 Solution Template	Monitors performance, availability, and usage statistics for Microsoft SQL Server 2005.
Microsoft Windows Host Solution Template	Monitors performance, availability, and health for Microsoft Windows 2000, Windows XP, and Windows Server 2003 host machines.
.NET Solution Templates	Monitors performance, availability, and health of .NET applications and environments on Windows 2000, Windows XP, and Windows Server 2003.
Oracle Database Solution Template	Monitors performance, availability, and usage statistics for Oracle 9i and 10g databases.
SAP Solution Templates	Monitors performance, availability, and usage statistics for SAP system components.
Siebel Solution Templates	Monitors performance, availability, and usage statistics for Siebel Application Server installed on Windows and UNIX operating systems.
Solaris Host Solution Templates	Monitors performance, availability, and health for Solaris host machines.
WebLogic Solution Template	Monitors performance, availability, and usage statistics for BEA WebLogic application servers.
WebSphere Solution Template	Monitors performance, availability, and usage statistics for IBM WebSphere Server 5.x application servers.

## Customizing Solution Templates

Since a solution template is unlikely to match all your system configurations, you can customize the solution template to meet your system requirements as follows:

- Copy the solution template to a template container, modify it to suit your system requirements, and then deploy the modified solution template.
- Deploy the solution template, and modify it after the deployment to suit your system's requirements.

For example, when using the HP Quality Center Application Server solution template to monitor the repository disk variable, and the repository is on a different host to the application server, after deploying the template, you must change the repository disk utilization monitor to use the other host.

## Notes and Limitations

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- After some solution templates are deployed, the relevant monitors may be defined with a BAC reporting level of **Disable reporting to BAC**. Therefore after deploying a solution template, we recommend that you check the monitors' reporting level. If you want to change the reporting level for the deployed monitors, you can use the Global Search and Replace wizard to update the reporting level option.
- Solution templates do not configure any automated alerts or reports for the monitors created. You may create and associate one or more alert definitions or reports to the monitors or monitor groups created by solution templates.

## Deploy a SiteScope Solution Template – Workflow

This task describes the steps involved in deploying a solution template. Deploy a solution template for each server in your environment.

This task includes the following steps:

- “Prerequisites” on page 1669
- “Deploy the Template” on page 1669
- “Enter Variable Values for the Template Deployment” on page 1670
- “Configure Alerts and Reports” on page 1670
- “Results” on page 1670

### 1 Prerequisites

- You must have the applicable SiteScope option license to use the Solution Template. Contact your HP sales representative for more information about Solution licensing.
- The license must be entered into **Monitor licenses** in **Preferences > General Preferences > Main Panel**. For details on the user interface, see “General Preferences User Interface” on page 1379.

### 2 Deploy the Template

Select the method for deploying the solution template to a group:

- You can deploy a solution template directly from the user interface. In the template tree, right-click the solution template you want to deploy, and select **Deploy Template**. In the Select Group dialog box, select the monitor group into which you want to deploy the solution template. For details on the Select Group user interface, see “Select Group Dialog Box” on page 1636.
- You can deploy a solution template using a CSV file that contains the variable values defined in the template. For details on this topic, see “Deploying a Template Using a CSV File” on page 1577. For details on how to perform this task, see “Deploy a Template Using a CSV File” on page 1592.

- ▶ You can also deploy and update the template using an XML file external to the SiteScope user interface. For details on this topic, see “Auto Template Deployment Overview” on page 1644.

### 3 Enter Variable Values for the Template Deployment

Complete the items on the Deployment Values page for the selected solution template. For details on the user interface, see the Deployment Values page for the specific solution template.

### 4 Configure Alerts and Reports

Configure alerts and reports for the newly created solution monitors.

For details on configuring alerts, see “Configure an Alert” on page 1984.

For details on configuring reports, see “Create a Report” on page 2041.

### 5 Results

The solution template creates a new monitor group container in which the individual solution monitors are added. The monitor group container is assigned a name in the format <Solution Template name> on <server\_name> where server\_name is the server selected from the **Server** box.

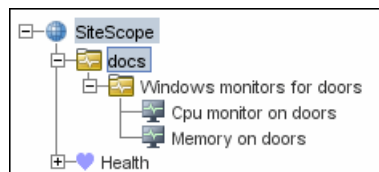
---

**Note:** If some of the monitors fail to deploy, a message is shown listing the names of the monitors together with a message describing the error.

---

You can view, edit, and delete these monitors in the same way as any other monitors in SiteScope.

#### Example




## Solution Template User Interface

### This section includes:

- Solution Templates Tree - Properties Tab on page 1671

## Solution Templates Tree - Properties Tab

<b>Description</b>	Displays the name and description of the selected solution template. <b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand the Solution Templates container and select the required template.
<b>Important Information</b>	<ul style="list-style-type: none"> <li>➤ Only licensed solution templates that are displayed with the  icon are configurable solution templates.</li> <li>➤ The Search/Filter Tags panel is not available for filtering Solution Template objects.</li> </ul>
<b>Included in Tasks</b>	“Deploy a SiteScope Solution Template – Workflow” on page 1669
<b>Useful Links</b>	“Template Tree” on page 84

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Name</b>	The solution template name (read-only).
<b>Description</b>	A description of the solution template (read-only).

## Troubleshooting and Limitations

The installed solution templates are located in the **<SiteScope root directory>\persistency** directory. If the contents of this directory are deleted, the solution templates no longer appear in the template tree. To reinstall the solution templates, you must copy the solution template files back to the **persistency** directory.

---

**Note:** We do not recommend deleting the **persistency** directory as this permanently deletes all SiteScope configuration data and all historic data in Business Availability Center (if SiteScope is integrated with HP Business Availability Center).

---

### To reinstall the solution template files:

- 1** Locate the solution template files in the following directory:  
**<SiteScope root directory>\export.**
- 2** Copy the contents of **<SiteScope root directory>\export** into **<SiteScope root directory>\persistency\import.**
- 3** Check that the solution templates have been reinstalled by locating them in the **Solution Templates** folder in the template tree.



# 134

---

## Active Directory Solution Template

This chapter includes the main concepts, tasks, and reference information for the Active Directory solution template.

### **This chapter includes:**

#### Concepts

- Active Directory Solution Overview on page 1673

#### Tasks

- Deploy the Active Directory Solution Template on page 1675

#### Reference

- Active Directory Solution Template User Interface on page 1676

### **Active Directory Solution Overview**

You can use the Active Directory solution template to provide monitoring of domain controller performance—services on which Active Directory depends—and distributed Active Directory performance.

The Active Directory solution template deploys a set of monitors against a particular Domain Controller. These monitors encompass best practices monitoring for Active Directory. This template includes NT Event Log, Service, LDAP, performance counter and Active Directory Replication monitors.

The Active Directory solution templates provide comprehensive monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the Active Directory solution templates. Contact your HP sales representative for more information about Solution licensing.
  - ▶ An in-depth description of the Active Directory Solution is available in the SiteScope Active Directory Best Practices document. This document is part of the SiteScope installation, and can be found at <**SiteScope root directory**>\sisdocs\pdfs\SiteScope\_Active\_Directory\_Best\_Practices.pdf. This is a password protected document. The password is provided along with the Active Directory Solution license key from HP.
- 

## **Solution Template Monitors**

The Active Directory solution template deploys monitors that target the following aspects of Active Directory performance:

- ▶ **Domain controller performance.** This category refers to the low level health of each domain controller in the environment. The Active Directory solution template automatically configures monitors for domain controller health.
- ▶ **Dependent services.** Active Directory depends on several key services. Without these services, Active Directory can become unresponsive or fail altogether. The Active Directory solution template automatically configures monitors for a list of important services on which Active Directory performance is dependent.

- **Distributed Active Directory performance.** Perhaps the most important aspect and key indicator of Active Directory performance is how fast Active Directory is replicating changes out to all domain controllers. The Active Directory solution template automatically configures monitors for monitoring and testing replication of changes and updates.

---

**Note:** Some of the monitor types deployed by the solution templates can only be added to SiteScope by using the Active Directory Solution sets. For more information, see the section for the particular monitor types.

---

## **Deploy the Active Directory Solution Template**

This task describes the steps involved in entering variables for the Active Directory solution template.

This task includes the following steps:

- “Deploy the Solution Template” on page 1675
- “Enter Deployment Values for the Solution Template” on page 1675

### **1 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **2 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the Active Directory solution template. For details on the user interface, see “Active Directory Solution Template User Interface” on page 1676.

## Active Directory Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the SiteScope Active Directory solution template.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select the required Active Directory solution template.</p>
<b>Included in Tasks</b>	“Deploy a SiteScope Solution Template – Workflow” on page 1669
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Active Directory Solution Template” on page 1673</li> <li>▶ “Template Tree” on page 84</li> </ul>

### Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>ReplicatingDomain Controllers</b>	Enter a comma separated list of domain controllers that replicate data from the domain controller selected above.
<b>LDAPSecurity Principal</b>	The LDAP Security Principal of a Domain Admin account. For Active Directory this is in the format of cn=Domain Admin User,cn=users,dc=yoursite,dc=com.
<b>LogicalDrive</b>	Enter the logical drive that this Domain Controller is using for its database and log files.
<b>PASSWORD</b>	The password for the user selected above.
<b>HostName</b>	Enter the host part of the domain controller's host name (do not include the fully qualified domain name).
<b>Global Catalog (AD with Global Catalog ONLY)</b>	If the Domain Controller is a Global Catalog server then check this box.

GUI Element	Description
<b>SERVER_LIST</b>	Choose the Domain Controller that you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server.
<b>Silent deployment</b>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to &lt;SiteScope root directory&gt;\logs\silent_deployment.log.</p> <p><b>Default value:</b> Not selected</p>
<b>Verify monitor properties with remote server</b>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>



# 135

---

## AIX Host Solution Templates

This chapter includes the main concepts, tasks, and reference information for the AIX Host solution template.

### **This chapter includes:**

#### **Concepts**

- ▶ AIX Host Solution Overview on page 1679

#### **Tasks**

- ▶ Deploy the AIX Host Solution Template on page 1681

#### **Reference**

- ▶ AIX Host Solution Configuration Requirements on page 1682
- ▶ AIX Host Solution Template User Interface on page 1682

### **AIX Host Solution Overview**

The AIX Host solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the AIX host. The template supports the versions of AIX that are supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can create a Server-Centric report which displays data from three different metrics about the server being monitored. We recommend that you use solution templates when creating the UNIX Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric report, see “Generating a Server-Centric Report” on page 1881.

The AIX Host solution template provides comprehensive AIX operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the AIX Host solution template. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the AIX Host Solutions settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at <**SiteScope root directory**>\sisdocs\pdfs\**SiteScope\_OS\_Best\_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

---

### **Solution Template Monitors**

The AIX Host solution template deploys monitors that target the following aspects of AIX performance and health:

- ▶ CPU status and utilization details
- ▶ Memory status and utilization details
- ▶ File system status and utilization details



## Deploy the AIX Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the AIX Host solution template.

---

**Note:** The AIX Host solution template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Server-Centric Report support.

---

This task includes the following steps:

- “Configure the AIX Server Environment” on page 1681
- “Deploy the Solution Template” on page 1681
- “Enter Deployment Values for the Solution Template” on page 1681

### **1 Configure the AIX Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “AIX Host Solution Configuration Requirements” on page 1682.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the AIX solution template. For details on the user interface, see “AIX Host Solution Template User Interface” on page 1682.

## AIX Host Solution Configuration Requirements

Before you can use the AIX Host solution template, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the target AIX host.
- The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test (**Remote Servers > UNIX Remote Servers**). For details, see “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285.
- The SiteScope server itself can also be monitoring if it runs a supported AIX operating system.
- The template supports the AIX versions supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

## AIX Host Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the SiteScope AIX solution template.</p> <p>Use this page to add the server monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select <b>AIX Host</b>.</p>
<b>Included in Tasks</b>	“Deploy a SiteScope Solution Template – Workflow” on page 1669
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “AIX Host Solution Templates” on page 1679</li> <li>➤ “Template Tree” on page 84</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>SERVER_LIST</b>	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a UNIX connection profile, see “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285.
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <SiteScope root directory>\logs\silent_deployment.log. <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected



# 136

---

## HP Quality Center Solution Templates

This chapter includes the main concepts, tasks, and reference information for the HP Quality Center solution templates.

### **This chapter includes:**

#### Concepts

- ▶ HP Quality Center Solution Templates Overview on page 1686

#### Tasks

- ▶ Deploy the HP Quality Center Solution Template on page 1689

#### Reference

- ▶ HP Quality Center Solution Template Configuration Requirements on page 1690
- ▶ HP Quality Center Solution Template User Interface on page 1692
- ▶ Troubleshooting and Limitations on page 1702

## HP Quality Center Solution Templates Overview

The HP Quality Center solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the availability of HP Quality Center 9.x and 10.x application servers, license status on HP Quality Center 9.2 and 10.0 database servers, and HP QuickTest Professional license server application and system availability.

The HP Quality Center solution templates provide comprehensive HP Quality Center monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy various performance monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the HP Quality Center solution templates. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the HP Quality Center Solution is available in the SiteScope Quality Center Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope\_HP\_QC\_Best\_Practices.pdf**. This is a password protected document. The password is provided along with the HP Quality Center Solution license key from HP.

---

This section includes:

- ▶ “Solution Template Monitors” on page 1687
- ▶ “Monitoring Quality Center Third Party Applications” on page 1687

## Solution Template Monitors

The HP Quality Center Solution includes solution templates for monitoring the following key components:

- **HP Quality Center Application Server for UNIX/Windows.** Use this solution template to monitor the availability and performance of the HP Quality Center application server on the operating system on which the application is installed.
- **HP Quality Center 9.2/10.0 License Status.** Use this solution template to monitor HP Quality Center license usage and expiration time on an HP Quality Center database server (the solution template has been certified on an Oracle and Microsoft SQL database).
- **HP QuickTest Professional License Server.** Use this solution template to monitor the availability and performance of the HP QuickTest Professional License Server.

## Monitoring Quality Center Third Party Applications

We recommend using other SiteScope solution templates and/or monitors to monitor Quality Center third party components, such as the application server on which Quality Center is deployed, and the database it uses.

For details on the solutions that are recommended for monitoring Quality Center third party components, see the tables below:

### Database Server Monitoring

Database Type	Recommended Solution
Oracle	"Oracle Database Solution Template" on page 1759
Microsoft SQL Server	"Microsoft SQL Server 2005 Solution Template" on page 1739
LDAP	"LDAP Monitor" on page 585

## Application/Web Server Monitoring

Application/Web Server Type	Recommended Solution
Apache Server	"Apache Server Monitor" on page 411
JBoss	"JBoss Application Server Solution Template" on page 1711
Microsoft IIS	"Microsoft IIS Solution Template" on page 1733 "Microsoft IIS Server Monitor" on page 665
WebLogic 6.x-8.x, 9.x-10.x	"WebLogic Solution Template" on page 1795
WebSphere 5.x, 6.x	"WebSphere Solution Template" on page 1805
Other Web/Application Servers that support JMX access (JSR 160)	"JMX Monitor" on page 577



## **Deploy the HP Quality Center Solution Template**

This task describes the steps involved in entering variables and deploying the HP Quality Center solution templates.

This task includes the following steps:

- “Configure the HP Quality Center Server Environment” on page 1689
- “Deploy the Solution Template” on page 1689
- “Enter Deployment Values for the Solution Template” on page 1689

### **1 Configure the HP Quality Center Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “HP Quality Center Solution Template Configuration Requirements” on page 1690.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the HP Quality Center solution template. For details on the user interface, see “HP Quality Center Solution Template User Interface” on page 1692.

## **HP Quality Center Solution Template Configuration Requirements**

Before you can use the HP Quality Center solution templates, there are a number of configuration requirements involving the server environment.

This section includes the following topics:

- ▶ “HP Quality Center Application Server for Windows” on page 1690
- ▶ “HP Quality Center Application Server for UNIX” on page 1691
- ▶ “HP Quality Center 9.2/10.0 License Status” on page 1691
- ▶ “HP QuickTest Professional License Server” on page 1692

### **HP Quality Center Application Server for Windows**

To deploy the HP Quality Center Application Server for Windows solution template:

- ▶ The SiteScope server must have access to the Quality Center components.
- ▶ You should have the following information:
  - ▶ Quality Center application version (9.2, 10.0)
  - ▶ Full host name and login credentials for the application server
  - ▶ Quality Center repository disk or repository location if it is located on another host
  - ▶ Port used in the login URL (usually none, which means that port 80 is used)

---

**Note:** This solution template is not supported on SiteScopes installed on UNIX platforms.

---

## HP Quality Center Application Server for UNIX

To deploy the HP Quality Center Application Server for UNIX solution template:

- ▶ The SiteScope server must have access to the Quality Center components.
- ▶ You should have the following information:
  - ▶ Quality Center application version (9.2, 10.0)
  - ▶ UNIX operating system type
  - ▶ Full host name and login credentials for the Application server
  - ▶ System file system
  - ▶ Quality Center repository disk or repository location if it is located on another host
  - ▶ Port used in the login URL (usually none, which means that port 80 is used)
  - ▶ Name of the java process command that runs the Quality Center application on the UNIX operating system. (you can use "ps -ef | grep java")

## HP Quality Center 9.2/10.0 License Status

To deploy the HP Quality Center 9.2/10.0 License Status solution template:

- ▶ The SiteScope server must have access to the Quality Center 9.2 or 10.0 components.
- ▶ You should have the following information on the Quality Center database:
  - ▶ Database host name
  - ▶ Type (Oracle, Microsoft SQL, MSDE 2000)
  - ▶ Driver (possibly a SiteScope built-in database driver)
  - ▶ Database Connection URL
  - ▶ Database user name and password

## HP QuickTest Professional License Server

To deploy the HP QuickTest Professional License Server solution template:

- ▶ The SiteScope server must have access to the QuickTest Professional License server.
- ▶ You should have the QuickTest Professional License server host name and login credentials.

---

**Note:** This solution template is not supported on SiteScopes installed on UNIX platforms.

---

## HP Quality Center Solution Template User Interface

<b>Description</b>	Enables you to deploy the HP Quality Center solution templates for monitoring the HP Quality Center 9.x and 10.x application servers on Windows and UNIX platforms, and license usage and expiration time on an HP Quality Center 9.2 or 10.0 database server. The templates also enable you to monitor HP QuickTest Professional license server application and system availability.  Use this page to add the server monitor or edit the monitor's properties.  <b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b> , and select the required HP Quality Center solution template.
<b>Important Information</b>	The solution template uses the Ping monitor to monitor system availability. If Ping traffic is blocked on your network, you should use Port monitor instead.

<b>Included in Tasks</b>	“Deploy a SiteScope Solution Template – Workflow” on page 1669
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “HP Quality Center Solution Templates Overview” on page 1686</li> <li>▶ “Troubleshooting and Limitations” on page 1702</li> <li>▶ “Template Tree” on page 84</li> </ul>

## HP Quality Center Application Server for Windows

The Main Settings include the following elements:

GUI Element	Description
<b>Application server host name</b>	The host name of the Quality Center application server.
<b>Application server user name</b>	The login user name for the host on the Quality Center application server.
<b>Application server password</b>	The password for the host on the Quality Center application server.
<b>System disk</b>	The logical disk drive where the Quality Center application server is installed. <b>Default value:</b> C
<b>Repository disk</b>	The logical disk drive where the Quality Center repository is located. If the repository is located on another host, enter the system disk drive and alter the Repository Disk Utilization monitor after you deploy your template. <b>Default value:</b> D
<b>Site Administration path</b>	The suffix for the Quality Center Site Administration URL. <b>Default value:</b> qcbn/SiteAdmin.htm. For Quality Center version 9.x, change this to sabin.

GUI Element	Description
<b>Application port</b>	<p>The port used in the login URLs to the Quality Center application. Usually no port is specified which means port 80 is used.</p> <p><b>Default value:</b> 80</p>
<b>Maximum round trip time (milliseconds)</b>	<p>The value in milliseconds, used as an error status threshold for a reasonable round trip time for getting a response from you application URLs.</p> <p><b>Default value:</b> 1500 milliseconds</p>
<b>Quality Center service name</b>	<p>The Quality Server service name.</p> <p><b>Default value:</b> HP Quality Center. For Quality Center version 9.x, change this to Mercury Quality Center.</p>
<b>Silent deployment</b>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to &lt;SiteScope root directory&gt;\logs\silent_deployment.log.</p> <p><b>Default value:</b> Not selected</p>
<b>Verify monitor properties with remote server</b>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>

## HP Quality Center Application Server for UNIX

The Main Settings include the following elements:

GUI Element	Description
<b>Application server host name</b>	The host name for the Quality Center application server.
<b>Application server user name</b>	The login user name for the host on the Quality Center application server.
<b>Application server password</b>	The password for the host on the Quality Center application server.
<b>UNIX operating system</b>	The UNIX operating system type, such as Sun Solaris, Red Hat Enterprise Linux. The complete list of UNIX operating system types is available in the <b>Operating system</b> field of the New/Edit UNIX Remote Server dialog box.  <b>Default value:</b> Linux
<b>System file system</b>	The file system where the Quality Center application is installed.
<b>Repository file system</b>	The file system where the Quality Center repository is located. If the repository is located on another host, enter the system disk file system, and alter the Repository Disk Utilization monitor after you deploy your template.
<b>Site Administration path</b>	The suffix for the Quality Center Site Administration URL.  <b>Default value:</b> qcbn/SiteAdmin.htm. For Quality Center version 9.x, change this to sabin.
<b>Application port</b>	The port used in the login URLs to the Quality Center application. Usually no port is specified which means port 80 is used.  <b>Default value:</b> 80

GUI Element	Description
<b>Maximum round trip time (milliseconds)</b>	<p>The value in milliseconds, used as an error status threshold for a reasonable round trip time for getting a response from you application URLs.</p> <p><b>Default value:</b> 1500 milliseconds</p>
<b>Quality Center process unique name</b>	<p>Name used to identify the Quality Center java process from the other processes running on the system. It can be the Quality Center process name, or a unique part of it taken from the java process command that runs the Quality Center application on the UNIX operating system (you can use <code>ps -ef   grep java</code>).</p>
<b>Silent deployment</b>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <code>&lt;SiteScope root directory&gt;\logs\silent_deployment.log</code>.</p> <p><b>Default value:</b> Not selected</p>
<b>Verify monitor properties with remote server</b>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>



## HP Quality Center 9.2/10.0 License Status

The Main Settings include the following elements:

GUI Element	Description
<b>Site Administration database host</b>	Host name where the Quality Center Site Administration is installed.
<b>Database driver</b>	<p>The database driver used for connecting to your database. If a custom driver is used, the driver must also be installed in the &lt;SiteScope root directory&gt;\WEB-INF\lib directory.</p> <p><b>Default value:</b> com.inet.ora.OraDriver (supports Oracle Database). For Microsoft SQL, use com.mercury.jdbc.sqlserver.SQLServerDriver.</p>
<b>Connection URL (full)</b>	<p>The Quality Center database connection URL.</p> <p><b>Examples:</b></p> <p>jdbc:inetora:[host]:[port]:[sid] (for Oracle Database)</p> <p>jdbc:mercury:sqlserver://labm1qcrnd05.devlab.ad:1433;DatabaseName=May22_2008_db (for Microsoft SQL)</p>
<b>Connection URL (part 0-3)</b>	<p>If your connection URL is composed of semicolon (;) separated values, enter each part in a separate field in addition to the full <b>Connection URL (full)</b> field.</p> <p><b>Example:</b></p> <p>Connection URL (part 0) = jdbc:mercury:sqlserver://labm1qcrnd05.devlab.ad:1433</p> <p>Connection URL (part 1) = DatabaseName=May22_2008_db</p> <p>Otherwise enter your whole connection URL in Connection URL (part 0) for example: Connection URL (part 0) = jdbc:inetora:[host]:[port]:[sid]</p> <p><b>Note:</b> The reason for this separation is that the connection URL is used as a Script monitor parameter, and the semicolon (;) character is not permitted for security reasons.</p>

GUI Element	Description
<b>Database user</b>	The user name required for querying the database. The specified user name must have privileges to run the SELECT queries on the ADMIN and SESSION_LICENSE tables of the Site Administration database.
<b>Database password</b>	The password required for the given user name to login to the database and run the SELECT queries.
<b>Database password - encrypted</b>	The encrypted form of the database password. To get the encrypted password, run the following tool on your password: <b>&lt;SiteScope root directory&gt;\tools\AutoDeployment\encrypt_password.bat &lt;password&gt;</b> For UNIX platforms, run <b>encrypt_password.sh &lt;password&gt;</b> . <b>Note:</b> The encrypted password is used as a Script monitor parameter, and is required for security reasons.
<b>Admin table name</b>	The name of the Quality Center ADMIN table. <b>Default value:</b> ADMIN (supports Oracle database). For Microsoft SQL database, use td.ADMIN.
<b>Session license table name</b>	The name of the Quality Center Session License table. <b>Default value:</b> SESSION_LICENSE (supports Oracle database). For Microsoft SQL database, use td.SESSION_LICENSE.
<b>SiteScope expiration error status (days remaining)</b>	This number is used as an error threshold. Each License Expiration Status deployed monitor is in error status if the number of days until the license expires is less than the number specified here. <b>Default value:</b> 7 days
<b>SiteScope expiration warning status (days remaining)</b>	This number is used as a warning threshold. Each License Expiration Status deployed monitor is in warning status if the number of days until the license expires is less than the number specified here. <b>Default value:</b> 30 days

GUI Element	Description
<b>Number of free licenses for error</b>	<p>This number is used as an error threshold. Each License Usage Status deployed monitor is in error status if the number of free licenses is less than the number specified here.</p> <p><b>Default value:</b> 5</p>
<b>Number of free licenses for warning</b>	<p>This number is used as an error threshold. Each License Usage Status deployed monitor is in warning status if the number of free licenses is less than the number specified here.</p> <p><b>Default value:</b> 20</p>
<b>Silent deployment</b>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to &lt;SiteScope root directory&gt;\logs\silent_deployment.log.</p> <p><b>Default value:</b> Not selected</p>
<b>Verify monitor properties with remote server</b>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>

**Note:**

- ▶ The Quality Center license is in XML format that is stored in the ADMIN table on the Site Administration database. It contains information about the Quality Center license expiration and quota for each of the different Quality Center modules (for example, Defects, Requirements, and so forth). The XML format is different for Quality Center 9.2 and Quality Center 10.0. Another table named SESSION\_LICENSE contains an entry on real time for each logged in session and the license type used.
  - ▶ To calculate the license usage and expiration, the SiteScope solution template uses a Script monitor that runs a script (**runQCLicenseTool.bat** on Microsoft Windows platforms, and **runQCLicenseTool.sh** on UNIX platforms). The script queries the Quality Center database, and returns the following information for the requested license type to the Script monitor:  
Total=<total quota>;used=<currently used of this type>;free=<total-free>;exp\_days=<left days for license to expire>.
-

## HP QuickTest Professional License Server

The Main Settings include the following elements:

GUI Element	Description
<b>QTP license server host name</b>	The host name for the QuickTest Professional license server.
<b>QTP license server user name</b>	The user name for the QuickTest Professional license server system login.
<b>QTP license server password</b>	The password for the QuickTest Professional license server system login.
<b>Silent deployment</b>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to &lt;SiteScope root directory&gt;\logs\<b>silent_deployment.log</b>.</p> <p><b>Default value:</b> Not selected</p>
<b>Verify monitor properties with remote server</b>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>

## Troubleshooting and Limitations

This section describes troubleshooting and limitations for the HP Quality Center 9.2/10.0 License Status solution template.

- If you encounter monitors that have a **content match error** after deploying the solution template, it is possible that your Quality Center does not support this type of license.

- If this is the case, you should delete the unsupported monitor.

- If the monitor is supported, you should check the log file:

- <SiteScope root directory>\scripts\qc\_license\_tool.log.

- To set the log file to debug, open <SiteScope root directory>\conf\ems\tools\conf\core\Tools\log4j\PlainJava\log4j.propeties

- and set

- loglevel=DEBUG

---

## HP Service Manager Solution Template

This chapter includes the main concepts, tasks, and reference information for the HP Service Manager solution template.

### **This chapter includes:**

#### Concepts

- ▶ HP Service Manager Solution Overview on page 1704

#### Tasks

- ▶ Deploy the HP Service Manager Solution Template on page 1705

#### Reference

- ▶ HP Service Manager Solution Configuration Requirements on page 1706
- ▶ HP Service Manager Solution Template User Interface on page 1707

## HP Service Manager Solution Overview

SiteScope's HP Service Manager solution template enables you to monitor and troubleshoot HP Service Manager application servers availability and system status on Windows and UNIX platforms. It measures HP Service Manager load balancer status, shared memory usage, and monitors logs for fatal errors. It can also be used to monitor HP Service Manager in Horizontal Scaled mode. The template supports Service Manager 7.11.

The HP Service Manager solution template provides comprehensive monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, and helps identify both real-time performance bottlenecks and longer term trends.

---

**Note:** You must have the applicable SiteScope option license to use the HP Service Manager solution template. Contact your HP sales representative for more information about Solution licensing.

---

### **Solution Template Monitors**

The HP Service Manager solution template creates a dynamic set of monitors that target the HP Service Manager server performance and health on Windows and UNIX platforms. For details on the monitors, see the SiteScope HP Service Manager Server Best Practices document.



## **Deploy the HP Service Manager Solution Template**

This task describes the steps involved in configuring the server environment and entering variables for the HP Service Manager solution template.

This task includes the following steps:

- “Configure the HP Service Manager Environment” on page 1705
- “Deploy the Solution Template” on page 1705
- “Enter Deployment Values for the Solution Template” on page 1705

### **1 Configure the HP Service Manager Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “HP Service Manager Solution Configuration Requirements” on page 1706.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the HP Service Manager solution template. For details on the user interface, see “HP Service Manager Solution Template User Interface” on page 1707.

## HP Service Manager Solution Configuration Requirements

Before you can use the HP Service Manager solution template, there are a number of configuration requirements involving the server environment:

- ▶ All processes to be monitored must be up and running when deploying the template.
- ▶ The HP Service Manager solution template supports Service Manager 7.11 only.
- ▶ For the HP Service Manager for Windows solution template, the **sm-lbstatus-win-ssh.bat** and **sm-shm-win-ssh.bat** scripts must be run on the Microsoft Windows remote server where HP Service Manager is installed. For details, see the task below.

---

**Note:** The HP Service Manager for UNIX solution template uses the **sm-shm.txt** and **sm-lbstatus.txt** files located in **<SiteScope root directory>/scripts.remote** to run commands on the remote Service Manager UNIX host.

---

### **Running the sm-lbstatus-win-ssh.bat and sm-shm-win-ssh.bat Scripts**

To run the scripts:

- 1** Install and configure the SSH Server (OpenSSH). For details, see “Configure Remote Windows Servers for SSH monitoring” on page 1325.
- 2** On the machine where SiteScope is installed, find the file called **RemoteNTSSH.zip** in the **<SiteScope root directory>\tools** directory. Unzip the **RemoteNTSSH.zip** file on the remote monitored Service Manager host. Place the contents of the zip file into the **C:\Documents and Settings\Administrator** folder.

- 3 On the machine where SiteScope is installed, find the file called **SM\_Scripts\_win\_ssh.zip** in the <SiteScope root directory>\tools\sm directory. Unzip the file on the remote monitored Service Manager host to C:\Documents and Settings\Administrator\scripts (The zip contains the sm-lbstatus-win-ssh.bat and sm-shm-win-ssh.bat files.) Make sure both scripts have execute permissions. If you are running Service Manager in Horizontally Scaled mode, you need to repeat this on every system.
- 4 Share the Service Manager logs folder. Right-click the **logs** folder and select **Properties > Sharing**. Select **Share this folder**, and enter a **Share name**. Set the share permissions for the user that SiteScope monitor uses to run the monitors on that machine, and click **OK**.

## HP Service Manager Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the HP Service Manager solution template.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select the required HP Service Manager solution template.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ If you are running HP Service Manager in Horizontally Scaled mode, you need to deploy and configure the HP Service Manager solution template on every system.</li> <li>▶ All processes to be monitored must be up and running when deploying the template. If you get a “no counters selected” error, it means that some processes are down. To resolve this problem, make a copy of the template and delete the monitors for which you get errors before deploying the template.</li> <li>▶ The solution template uses the Ping monitor to monitor system availability. If Ping traffic is blocked on your network, you should use the Port monitor, and use Global Search and Replace to replace the dependency from the Ping monitor to the Port monitor.</li> </ul>

<b>Included in Tasks</b>	“Deploy a SiteScope Solution Template – Workflow” on page 1669
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “HP Service Manager Solution Template” on page 1703</li> <li>➤ “Template Tree” on page 84</li> </ul>

## HP Service Manager for Windows

The Main Settings include the following elements:

GUI Element	Description
<b>SM installation partition</b>	Enter the disk drive where HP Service Manager is installed. <b>Default value:</b> C
<b>Application server host name</b>	Enter the name of the application server host.
<b>User name</b>	Enter the login name to access the application server using this profile.
<b>Password</b>	Enter the application server login password for this user.
<b>Installation path</b>	Enter the path to the directory on which HP Service Manager binary is running. <b>Default value:</b> C:\Program Files\HP\Service Manager 7.11\Server\RUN
<b>CPU error threshold</b>	The threshold for triggering CPU errors. <b>Default value:</b> 90
<b>CPU warning threshold</b>	The threshold for triggering CPU warnings. <b>Default value:</b> 80
<b>Memory error threshold</b>	The threshold for triggering memory errors. <b>Default value:</b> 2202012 KB
<b>Memory warning threshold</b>	The threshold for triggering memory warnings. <b>Default value:</b> 1782580 KB

GUI Element	Description
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <SiteScope root directory>\logs\silent_deployment.log. <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected

## HP Service Manager for UNIX - Main Settings

The Main Settings include the following elements:

GUI Element	Description
<b>SM installation partition</b>	Enter the disk drive where HP Service Manager is installed.
<b>Application server host name</b>	Enter the name of the application server host.
<b>User name</b>	Enter the login name to access the application server using this profile.
<b>Password</b>	Enter the application server login password for this user.
<b>UNIX operating system</b>	Enter the UNIX operating system on which HP Service Manager is running.
<b>UNIX connection method</b>	Enter the method used to connect to the UNIX operating system.

GUI Element	Description
<b>Shell prompt</b>	Enter the prompt output when the remote system is ready to handle a command (for Telnet or Rlogin connection method only).
<b>Installation path</b>	Enter the path to the directory on which HP Service Manager binary is running.
<b>CPU error threshold</b>	The threshold for triggering CPU errors. <b>Default value:</b> 90
<b>CPU warning threshold</b>	The threshold for triggering CPU warnings. <b>Default value:</b> 80
<b>Memory error threshold</b>	The threshold for triggering memory errors. <b>Default value:</b> 2202012 KB
<b>Memory warning threshold</b>	The threshold for triggering memory warnings. <b>Default value:</b> 1782580 KB
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <SiteScope root directory>\logs\silent_deployment.log. <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected

# 138

---

## JBoss Application Server Solution Template

This chapter includes the main concepts, tasks, and reference information for the JBoss Application Server solution template.

### **This chapter includes:**

#### Concepts

- JBoss Application Server Solution Overview on page 1712

#### Tasks

- Deploy the JBoss Application Server Solution Template on page 1713

#### Reference

- JBoss Solution Configuration Requirements on page 1714
- JBoss Solution Template User Interface on page 1715

## JBoss Application Server Solution Overview

The JBoss Application Server solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of JBoss application servers. The template supports JBoss Application Server versions 4.0.x and 4.2.x.

The JBoss Application Server solution template provides comprehensive JBoss monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

---

### Note:

- ▶ You must have the applicable SiteScope option license to use the JBoss Application Server solution template. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the JBoss solution is available in the SiteScope JBoss Application Server Best Practices document. This document can be found at <SiteScope root directory>\sisdocs\pdfs\**SiteScope\_JBoss\_Best\_Practices.pdf**. This is a password protected document. The password is provided along with the JBoss Application Server solution license key from HP.

---

### Solution Template Monitors

The JBoss Application Server solution template creates a dynamic set of monitors that target the JBoss application server performance and health. The exact monitor set depends on the entities you select during the solution template deployment. For details on the monitors, see the SiteScope JBoss Application Server Best Practices document.



## **Deploy the JBoss Application Server Solution Template**

This task describes the steps involved in configuring the server environment and entering variables for the JBoss Application Server solution template.

This task includes the following steps:

- “Configure the JBoss Server Environment” on page 1713
- “Deploy the Solution Template” on page 1713
- “Enter Deployment Values for the Solution Template” on page 1713

### **1 Configure the JBoss Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “JBoss Solution Configuration Requirements” on page 1714.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the JBoss Application Server solution template. For details on the user interface, see “JBoss Solution Template User Interface” on page 1715.

## JBoss Solution Configuration Requirements

Before you can use the JBoss Application Server solution, there are a number of configuration requirements involving the server environment:

- ▶ You must know the URL for gathering JMX statistics (including the host name and port of the JMX instance), and the JMX user name and password.
- ▶ SiteScope and the target server can run on the same host.
- ▶ The JBoss solution template supports JBoss application servers 4.0.x and 4.2.x only.
- ▶ You must start JBoss in a particular way, so that SiteScope is able to monitor it. For details, see “Starting JBoss” below.

### Starting JBoss

To enable SiteScope to monitor JBoss, you should specify the following options for the JBoss JVM:

```
-Dcom.sun.management.jmxremote.port=12345 (any other port can be used of course;
then it must be specified during ST deployment)
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false
-Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServer
BuilderImpl
-Djboss.platform.mbeanserver
-Dcom.sun.management.jmxremote
```

You can perform this using the following batch file:

```
@echo off
set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.port=12345
set JAVA_OPTS=%JAVA_OPTS% -
Dcom.sun.management.jmxremote.authenticate=false
set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.ssl=false
set JAVA_OPTS=%JAVA_OPTS% -
Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServer
BuilderImpl
set JAVA_OPTS=%JAVA_OPTS% -Djboss.platform.mbeanserver
set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote
call run.bat -b my-jboss-host
```

**Note:**

- ▶ **run.bat** is the default script used to start JBoss.
- ▶ **-b** option binds JBoss 4.2.2 to the correct network interface (it binds only to localhost by default making it inaccessible from other hosts).
- ▶ You can build a similar script for UNIX.

## **JBoss Solution Template User Interface**

<b>Description</b>	<p>Enables you to deploy the JBoss Application Server solution template.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select <b>JBoss AS 4.x</b>.</p>
<b>Included in Tasks</b>	<p>"Deploy a SiteScope Solution Template – Workflow" on page 1669</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ "JBoss Application Server Solution Template" on page 1711</li> <li>▶ "Template Tree" on page 84</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>JMX_URL</b>	The URL to gather JMX statistics. Typically the URL is in the format: service:jmx:rmi:///jndi/rmi://{hostname}:{port}/jmxrmi. Enter the host name and port of the JMX instance you want to monitor.
<b>USERNAME</b>	User name for connection to the JMX application (optional).
<b>Password</b>	Password for connection to the JMX application (optional).
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the entities you want to monitor. For each instance, a specific set of monitors and thresholds is created. For details, see the SiteScope JBoss Application Server Best Practices Guide which can be found at <SiteScope root directory>\sisdocs\pdfs\ <b>SiteScope_JBoss_Best_Practices.pdf.</b>

GUI Element	Description
<b>Silent deployment</b>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <b>&lt;SiteScope root directory&gt;\logs\silent_deployment.log</b>.</p> <p><b>Default value:</b> Not selected</p>
<b>Verify monitor properties with remote server</b>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>



# 139

---

## Linux Host Solution Templates

This chapter includes the main concepts, tasks, and reference information for the Linux Host solution template.

### **This chapter includes:**

#### Concepts

- ▶ Linux Host Solution Overview on page 1719

#### Tasks

- ▶ Deploy the Linux Host Solution Template on page 1721

#### Reference

- ▶ Linux Host Solution Configuration Requirements on page 1722
- ▶ Linux Host Solution Template User Interface on page 1722

### **Linux Host Solution Overview**

The Linux Host solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the target Linux host. The template supports the versions of Linux that are supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can create a Server-Centric report which displays data from three different metrics about the server being monitored. We recommend that you use solution templates when creating the UNIX Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric report, see “Generating a Server-Centric Report” on page 1881.

The Linux Host solution template provides comprehensive Linux operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the Linux Host solution template. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the Linux Host Solutions settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at <**SiteScope root directory**>\sisdocs\pdfs\**SiteScope\_OS\_Best\_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

---

## **Solution Template Monitors**

The Linux Host solution template deploys monitors that target the following aspects of Linux performance and health:

- ▶ CPU status and utilization details
- ▶ Memory status and utilization details
- ▶ File system status and utilization details



## Deploy the Linux Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Linux Host solution template.

---

**Note:** The Linux Host solution template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Server-Centric Report support.

---

This task includes the following steps:

- “Configure the Linux Server Environment” on page 1721
- “Deploy the Solution Template” on page 1721
- “Enter Deployment Values for the Solution Template” on page 1721

### **1 Configure the Linux Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “Linux Host Solution Configuration Requirements” on page 1722.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the Linux Host solution template. For details on the user interface, see “Linux Host Solution Template User Interface” on page 1722.

## Linux Host Solution Configuration Requirements

Before you can use the Linux Host solution template, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the target Linux host.
- The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test (**Remote Servers > UNIX Remote Servers**). For details, see “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285.
- The SiteScope server itself can also be monitoring if it runs a supported Linux operating system.
- The template supports the Linux versions supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

## Linux Host Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the Linux Host solution template. Use this page to add the server monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select <b>Linux Host</b>.</p>
<b>Included in Tasks</b>	<p>“Deploy a SiteScope Solution Template – Workflow” on page 1669</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Linux Host Solution Templates” on page 1719</li> <li>➤ “Template Tree” on page 84</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>SERVER_LIST</b>	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a UNIX connection profile, see “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285.
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <b>&lt;SiteScope root directory&gt;\logs\silent_deployment.log</b> . <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected



---

## Microsoft Exchange Solution Templates

This chapter includes the main concepts, tasks, and reference information for the Microsoft Exchange solution templates.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft Exchange Solution Overview on page 1726

#### Tasks

- ▶ Deploy Microsoft Exchange Solution Templates on page 1728

#### Reference

- ▶ Microsoft Exchange Solution Configuration Requirements on page 1729
- ▶ Microsoft Exchange Solution Template User Interface on page 1729

## Microsoft Exchange Solution Overview

The Microsoft Exchange solution templates provide monitoring of performance, availability, and usage statistics for:

- ▶ Microsoft Exchange 5.5 Server
- ▶ Microsoft Exchange 2000 Server
- ▶ Microsoft Exchange 2003 Server
- ▶ Microsoft Exchange 2007 Server (version 8.0)

Depending on the set chosen, this set includes monitors checking NT Event log entries, MAPI operations, system performance counters, and message system usage statistics.

The Microsoft Exchange solution templates provide comprehensive Microsoft Exchange system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the Microsoft Exchange solution templates. Contact your HP sales representative for more information about Solution licensing.
  - ▶ An in-depth description of the Microsoft Exchange Solution is available in the SiteScope Microsoft Exchange Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope\_Exchange\_Best\_Practices.pdf**. This is a password protected document. The password is provided along with the Microsoft Exchange Solution license key from HP.
-

## Solution Template Monitors

The Microsoft Exchange solution templates deploy monitors that target the following aspects of Microsoft Exchange performance and health:

- ▶ **Basic server/OS performance.** This category refers to the system-level health of a server. The Microsoft Exchange solution templates automatically configure monitors for server health.
- ▶ **Application performance.** Application performance is a measure of how well specific Exchange components are functioning. The Microsoft Exchange solution templates automatically configure monitors for a list of important Exchange application components.
- ▶ **Mail protocol response time.** Perhaps the most important aspect and key indicator of Microsoft Exchange performance is mail protocol response time. While Microsoft Exchange can utilize many protocols, the MAPI protocol is commonly used in Microsoft networks.
- ▶ **Usage statistics.** The last category related to Microsoft Exchange performance is usage. While usage in and of itself is not necessarily a key indicator of performance, changes in usage can affect overall Microsoft Exchange performance. In addition, Microsoft Exchange usage statistics help IT organizations spot trends and plan for the future. The Microsoft Exchange solution templates automatically configure monitors for a list of important Microsoft Exchange usage parameters.

---

**Note:** Some of the monitor types deployed by the solution templates can only be added to SiteScope by using the Microsoft Exchange solution templates. See the section for the particular monitor types for more information.

---

## **Deploy Microsoft Exchange Solution Templates**

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft Exchange solution template.

This task includes the following steps:

- “Configure the Microsoft Exchange Server Environment” on page 1728
- “Deploy the Solution Template” on page 1728
- “Enter Deployment Values for the Solution Template” on page 1728

### **1 Configure the Microsoft Exchange Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “Microsoft Exchange Solution Configuration Requirements” on page 1729.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the Microsoft Exchange solution template. For details on the user interface, see “Microsoft Exchange Solution Template User Interface” on page 1729.



## Microsoft Exchange Solution Configuration Requirements

Before deploying a Microsoft Exchange solution template, you must perform various steps depending on the solution template you want to deploy.

- ▶ **Microsoft Exchange 5.5, 2000, 2003 solutions.** These solution templates make use of the SiteScope MAPI Monitor. Successful deployment of this monitor type requires specific setup configuration relating to the mailbox owners and the SiteScope service. For the MAPI Monitor system requirements, see “MAPI Monitor Overview” on page 614.
- ▶ **Microsoft Exchange 2007 solution.** The Microsoft Exchange 2007 solution template makes use of the Microsoft Exchange 2007 Monitor. Successful deployment of this monitor type requires specific setup configuration as described in “Microsoft Exchange 2007 Monitor Overview” on page 645.

## Microsoft Exchange Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the Microsoft Exchange solution templates for monitoring:</p> <ul style="list-style-type: none"> <li>▶ Microsoft Exchange 5.5 Servers</li> <li>▶ Microsoft Exchange 2000 Servers</li> <li>▶ Microsoft Exchange 2003 Servers</li> <li>▶ Microsoft Exchange 2007 Servers (version 8.0)</li> </ul> <p>Use this page to add the server monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select the required Microsoft Exchange solution template.</p>
<b>Included in Tasks</b>	<p>“Deploy a SiteScope Solution Template – Workflow” on page 1669</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Microsoft Exchange Solution Templates” on page 1725</li> <li>▶ “Template Tree” on page 84</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>MailBox</b>	The name (alias) of the mailbox to be used for testing email round trip times using MAPI. This is often the email account name but it may be a different name. We recommend that you copy the mailbox name as it appears in the E-Mail Account properties for the email account you are using for this solution.
<b>MailUser</b>	The Windows account login name for the user for which email round trip times is tested using MAPI.
<b>MailDomain (on Microsoft Exchange 5.5, 2000, and 2003)</b> <b>Domain (on Exchange 2007)</b>	The domain to which both the owner of the mailbox being used and the Microsoft Exchange server belong. <b>Note:</b> The owner of the mailbox to be used by this solution must also have administrative account privileges on the machine where SiteScope is running. SiteScope also needs user account access to the domain where the Microsoft Exchange server is running.
<b>MAILPASSWORD</b>	The Windows account login password for the user name entered above.
<b>SERVER_LIST</b>	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
<b>AuthenticationUser (Microsoft Exchange 2003 only)</b>	The user name to use when querying the server for mailbox and public folder statistics. The statistics are gathered by using WMI (Windows Management Instrumentation), so the user name entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2. If this box is left blank, the user that SiteScope is running as is used.

GUI Element	Description
<b>AUTHENTICATION PASSWORD (Microsoft Exchange 2003 only)</b>	The password for the user entered above for gathering WMI statistics, or leave this blank if the user box is left blank.
<b>PSConsoleFile (Microsoft Exchange 2007 only)</b>	The path to the Microsoft Exchange Management Shell PowerShell console file.
<b>Silent deployment</b>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to &lt;SiteScope root directory&gt;\logs\silent_deployment.log.</p> <p><b>Default value:</b> Not selected</p>
<b>Verify monitor properties with remote server</b>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>



---

## Microsoft IIS Solution Template

This chapter includes the main concepts, tasks, and reference information for the Microsoft IIS solution template.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft IIS Solution Overview on page 1734

#### Tasks

- ▶ Deploy the Microsoft IIS Solution Template on page 1735

#### Reference

- ▶ Microsoft IIS Solution Configuration Requirements on page 1736
- ▶ Microsoft IIS Solution Template User Interface on page 1736

## Microsoft IIS Solution Overview

The Microsoft IIS solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of Microsoft IIS servers. The template supports Microsoft IIS 6.0 server.

The Microsoft IIS solution template provides comprehensive IIS monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

---

### Note:

- ▶ You must have the applicable SiteScope option license to use the Microsoft IIS solution template. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the IIS solution is available in the SiteScope Microsoft IIS Best Practices document. This document can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_IIS_Best_Practices.pdf`. This is a password protected document. The password is provided along with the IIS solution license key from HP.

---

### Solution Template Monitors

The Microsoft IIS solution template deploys monitors that target the following services and aspects of IIS server performance and health:

- ▶ Active Server Pages (ASP errors, requests, templates, sessions, transactions)
- ▶ FTP service, Web service, SMTP server, NNTP server, HTTP/HTTPS services, MSMQ Queue service, IIS Server, Global IIS status, Indexing services
- ▶ IIS statistics as a Windows process

## **Deploy the Microsoft IIS Solution Template**

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft IIS solution template.

This task includes the following steps:

- “Configure the Microsoft IIS Server Environment” on page 1735
- “Deploy the Solution Template” on page 1735
- “Enter Deployment Values for the Solution Template” on page 1735

### **1 Configure the Microsoft IIS Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “Microsoft IIS Solution Configuration Requirements” on page 1736.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the Microsoft IIS solution template. For details on the user interface, see “Microsoft IIS Solution Template User Interface” on page 1736.

## Microsoft IIS Solution Configuration Requirements

Before you can use the Microsoft IIS solution, there are a number of configuration requirements involving the server environment:

- ▶ SiteScope server must be able to connect to the target Microsoft IIS host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see “Microsoft Windows Resources Monitor Overview” on page 714.
- ▶ The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Remote Servers > Microsoft Windows Remote Servers**). For details, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291. Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, See “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
- ▶ SiteScope and the target Microsoft IIS server can run on the same host.

## Microsoft IIS Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the Microsoft IIS 6 solution template.</p> <p>Use this page to add the server monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select <b>Microsoft IIS 6</b>.</p>
<b>Included in Tasks</b>	<p>“Deploy a SiteScope Solution Template – Workflow” on page 1669</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Microsoft IIS Solution Template” on page 1733</li> <li>▶ “Template Tree” on page 84</li> </ul>



## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>SERVER_LIST</b>	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <b>&lt;SiteScope root directory&gt;\logs\silent_deployment.log</b> . <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected



# 142

---

## Microsoft SQL Server 2005 Solution Template

This chapter includes the main concepts, tasks, and reference information for the Microsoft SQL Server solution template.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft SQL Server 2005 Solution Overview on page 1739

#### Tasks

- ▶ Deploy the Microsoft SQL Server 2005 Solution Template on page 1741

#### Reference

- ▶ Microsoft SQL Server 2005 Solution Configuration Requirements on page 1742
- ▶ Microsoft SQL Server 2005 Solution Template User Interface on page 1743

### **Microsoft SQL Server 2005 Solution Overview**

The Microsoft SQL Server solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of Microsoft SQL servers. The template supports Microsoft SQL Server 2005 and 2008.

The Microsoft SQL Server solution template provides comprehensive Microsoft SQL server monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the Microsoft SQL Server solution template. Contact your HP sales representative for more information about Solution licensing.
  - ▶ An in-depth description of the Microsoft SQL Server solution is available in the SiteScope Microsoft SQL Server Best Practices document. This document can be found at <SiteScope root directory>\sisdocs\pdfs\**SiteScope\_MSSQL\_Best\_Practices.pdf**. This is a password protected document. The password is provided along with the Microsoft SQL Server solution license key from HP.
- 

### **Solution Template Monitors**

The Microsoft SQL Server solution template deploys monitors that target the following aspects of Microsoft SQL server performance and health:

- ▶ CPU status and utilization details
- ▶ Memory status and utilization details
- ▶ Disk utilization information
- ▶ SQL Server objects (Buffer Manager, Databases, Locks, Transactions)
- ▶ SQL Server resources (space available, percentage of currently connected users)

The Microsoft SQL Server solution makes use of the SiteScope Database Counter monitor, Microsoft SQL Server monitor, and Microsoft Windows Resources monitor. For detailed information about these monitors, see “Database Counter Monitor Overview” on page 467, “Microsoft SQL Server Monitor Overview” on page 672, and “Microsoft Windows Resources Monitor Overview” on page 714.

## **Deploy the Microsoft SQL Server 2005 Solution Template**

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft SQL Server 2005 solution template.

This task includes the following steps:

- “Configure the Microsoft SQL Server Environment” on page 1741
- “Deploy the Solution Template” on page 1741
- “Enter Deployment Values for the Solution Template” on page 1741

### **1 Configure the Microsoft SQL Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “Microsoft SQL Server 2005 Solution Configuration Requirements” on page 1742.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the Microsoft SQL Server 2005 solution template. For details on the user interface, see “Microsoft SQL Server 2005 Solution Template User Interface” on page 1743.

## Microsoft SQL Server 2005 Solution Configuration Requirements

Before you can use the Microsoft SQL Server solution, there are a number of configuration requirements involving the server environment:

- ▶ SiteScope server must be able to connect to the target Microsoft SQL host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see “Microsoft Windows Resources Monitor Overview” on page 714.
- ▶ The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Remote Servers > Microsoft Windows Remote Servers**). For details, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291. Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, See “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
- ▶ The SQL Server user must have **VIEW SERVER STATE** permissions on the monitored SQL Server 2005 instance to retrieve data from SQL Server System Views. For more information about granting permissions on Microsoft SQL Server 2005, see <http://msdn2.microsoft.com/en-us/library/ms186717.aspx>.
- ▶ SiteScope and the target Microsoft SQL Server can run on the same host.

## Microsoft SQL Server 2005 Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the Microsoft SQL Server 2005 solution template for monitoring key components on Microsoft SQL Server 2005.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select <b>Microsoft SQL Server 2005</b>.</p>
<b>Included in Tasks</b>	<p>"Deploy a SiteScope Solution Template – Workflow" on page 1669</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ "Microsoft SQL Server 2005 Solution Template" on page 1739</li> <li>▶ "Template Tree" on page 84</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Login to Microsoft SQL Server 2005</b>	The login name for the user on the monitored Microsoft SQL Server 2005 instance.
<b>Microsoft SQL Server 2005 password</b>	The password for the user on the monitored Microsoft SQL Server 2005 instance.
<b>Microsoft SQL Server 2005 URL</b>	<p>The URL for the monitored Microsoft SQL Server 2005 instance.</p> <ul style="list-style-type: none"> <li>▶ Replace <code>\${host}</code> with the host name on which the Microsoft SQL Server 2005 is running. This must be the same as the host name defined for the Windows remote machine. For details, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291.</li> <li>▶ Replace <code>\${port}</code> with the port number on which the Microsoft SQL Server 2005 accepts connections. By default, the port is 1433.</li> </ul> <p><b>Example:</b> <code>jdbc:mercury:sqlserver://doors:1433</code></p>



GUI Element	Description
<b>SERVER_LIST</b>	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <SiteScope root directory>\logs\silent_deployment.log. <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected



# 143

---

## Microsoft Windows Host Solution Template

This chapter includes the main concepts, tasks, and reference information for the Microsoft Windows Host solution template.

### **This chapter includes:**

#### Concepts

- ▶ Microsoft Windows Host Solution Overview on page 1747

#### Tasks

- ▶ Deploy the Microsoft Windows Host Solution Template on page 1749

#### Reference

- ▶ Microsoft Windows Host Solution Configuration Requirements on page 1750
- ▶ Microsoft Windows Host Solution Template User Interface on page 1751

### **Microsoft Windows Host Solution Overview**

The Microsoft Windows Host solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the Windows host. The template supports Microsoft Windows 2000, Windows XP, and Windows Server 2003.

For Microsoft Windows Resource Monitors, you can create a Server-Centric report which displays data from three different metrics about the server being monitored. We recommend that you use solution templates when creating the Microsoft Windows Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric report, see “Generating a Server-Centric Report” on page 1881.

The Microsoft Windows Host solution template provides comprehensive Windows operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the Microsoft Windows Host solution template. Contact your HP sales representative for more information about Solution licensing.
- ▶ An in-depth description of the Microsoft Windows Host Solution settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_OS_Best_Practices.pdf`. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

---

### **Solution Template Monitors**

The Microsoft Windows Host solution template deploys monitors that target the following aspects of Microsoft Windows performance and health:

- ▶ High-level CPU status and utilization details
- ▶ High-level Memory status and utilization details
- ▶ Disk utilization information

## Deploy the Microsoft Windows Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft Windows Host solution template.

---

**Note:** The Microsoft Windows Host Solution deploys a Microsoft Windows Resource Monitor for each target host. This monitor is an additional monitor that is required for Server-Centric Report support.

---

This task includes the following steps:

- “Configure the Microsoft Windows Server Environment” on page 1749
- “Deploy the Solution Template” on page 1749
- “Enter Deployment Values for the Solution Template” on page 1749

### **1 Configure the Microsoft Windows Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “Microsoft Windows Host Solution Configuration Requirements” on page 1750.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the Microsoft Windows Host solution template. For details on the user interface, see “Microsoft Windows Host Solution Template User Interface” on page 1751.

## Microsoft Windows Host Solution Configuration Requirements

Before you can use the Microsoft Windows Host Solution, there are a number of configuration requirements involving the server environment:

- ▶ SiteScope server must be able to connect to the target Windows host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see “Microsoft Windows Resources Monitor Overview” on page 714.
- ▶ The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Remote Servers > Microsoft Windows Remote Servers**). For details, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291. Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, See “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
- ▶ You can monitor Windows operating system usage statistics on the SiteScope server provided SiteScope is installed on a supported Windows operating system. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.
- ▶ SiteScope and the target server can run on the same host if SiteScope is installed on a Windows operating system supported by the template. The template supports Microsoft Windows 2000, Windows XP, and Windows Server 2003.

## Microsoft Windows Host Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the Microsoft Windows Host solution template for monitoring a Microsoft Windows 2000, Windows XP, and Windows Server 2003 operating system.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select <b>Microsoft Windows Host</b>.</p>
<b>Included in Tasks</b>	<p>"Deploy a SiteScope Solution Template – Workflow" on page 1669</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ "Microsoft Windows Host Solution Template" on page 1747</li> <li>▶ "Template Tree" on page 84</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>SERVER_LIST</b>	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <b>&lt;SiteScope root directory&gt;\logs\silent_deployment.log</b> . <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected



---

## .NET Solution Templates

This chapter includes the main concepts, tasks, and reference information for the .NET solution templates.

### **This chapter includes:**

#### Concepts

- ▶ .NET Solution Overview on page 1753

#### Tasks

- ▶ Deploy the .NET Solution Template on page 1755

#### Reference

- ▶ .NET Solution Configuration Requirements on page 1756
- ▶ .NET Solution Template User Interface on page 1756

### .NET Solution Overview

The .NET solution templates enable you to monitor .NET applications of servers that run a Windows operating system. This solution template deploys a set of monitors that test the health, availability, and performance of a .NET application and .NET environment on the Windows host. The template supports Windows 2000, Windows XP, and Windows Server 2003.

The .NET solution templates provide comprehensive .NET monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the .NET solution templates. Contact your HP sales representative for more information about Solution licensing.
  - ▶ An in-depth description of the .NET Solution is available in the SiteScope .NET Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope.NET.Best\_Practices.pdf**. This is a password protected document. The password is provided along with the .NET Solution license key from HP.
- 

## **Solution Template Monitors**

The .NET solution templates deploy monitors that target the following aspects of .NET performance and health:

- ▶ **.NET CLR Data.** This category refers to the common language runtime data (environment of .NET applications). It is designed to check several resource statistics for the .NET CLR for selected application. The .NET solution template automatically configures monitors for server health.
- ▶ **ASP.NET.** This category is designed to check several resource statistics for the ASP.NET. It gathers common information about application restarts and whole ASP.NET system stability. The .NET solution template automatically configures monitors for server health.
- ▶ **ASP.NET Applications.** This category is designed to check several resource statistics for the selected ASP.NET application. It gathers common information about application cache, errors, and other critical information. The .NET solution template automatically configures monitors for server health.

## Deploy the .NET Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the .NET solution template.

This task includes the following steps:

- “Configure the .NET Server Environment” on page 1755
- “Deploy the Solution Template” on page 1755
- “Enter Deployment Values for the Solution Template” on page 1755

### **1 Configure the .NET Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “.NET Solution Configuration Requirements” on page 1756.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the .NET solution template. For details on the user interface, see “.NET Solution Template User Interface” on page 1756.

## .NET Solution Configuration Requirements

Before you can use the .NET Solution, there are a number of configuration requirements involving the server environment:

- ▶ SiteScope server must be able to connect to the target Windows host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see “Microsoft Windows Resources Monitor Overview” on page 714.
- ▶ The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Remote Servers > Microsoft Windows Remote Servers**). For details, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291. Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, See “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277.
- ▶ SiteScope and the target .NET application can run on the same host if SiteScope is installed on a Windows operating system supported by the template. The template supports Windows 2000, Windows XP, and Windows Server 2003.

## .NET Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the .Net solution template for monitoring .NET application and .NET environments.</p> <p>Use this page to add the server monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select the required .NET solution template.</p>
<b>Included in Tasks</b>	<p>“Deploy a SiteScope Solution Template – Workflow” on page 1669</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “.NET Solution Templates” on page 1753</li> <li>▶ “Template Tree” on page 84</li> </ul>

## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Server</b>	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. See “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277 for the steps you use to create a Windows connection profile.
<b>ASP.NET Application (ASP.NET Application only)</b>	The name of the ASP.NET application you want to monitor. The name must be as it appears in the Task Manager.
<b>Instance (.NET CLR Data only)</b>	The name of the application you want to monitor. The name must be the same as it appears in the Task Manager, or can be whole system statistics (by default).
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <b>&lt;SiteScope root directory&gt;\logs\silent_deployment.log</b> . <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected



# 145

---

## Oracle Database Solution Template

This chapter includes the main concepts, tasks, and reference information for the Oracle Database solution templates.

### **This chapter includes:**

#### **Concepts**

- ▶ Oracle Database Solution Overview on page 1760

#### **Tasks**

- ▶ Deploy Oracle Database Solution Templates on page 1762

#### **Reference**

- ▶ Oracle Database Solution Template Usage Guidelines on page 1763
- ▶ Oracle Database Solution Template Tools on page 1763
- ▶ Oracle Solution Template User Interface on page 1766

## Oracle Database Solution Overview

You can use the Oracle Database solution templates to deploy a set of monitors that test the health, availability, and performance of an Oracle database. The deployed monitors check general system statistics, such as cache hit ratios and disk I/O, and include tools that provide diagnostic information about important aspects of the database. This solution can be used with Oracle 9, 10g, and 11g databases.

This solution uses the Database Counter Monitor to collect performance metrics from JDBC-accessible databases. In addition, you can use the Oracle Database solution template to deploy a collection of monitors configured with default metrics.

Important system metrics are computed with data retrieved from system tables in the Oracle database. A wide range of Oracle system tables such as V\$SYSSTAT, V\$LATCH, V\$ROLL\_STAT, and V\$BUFFER\_POOL\_STATISTICS are consulted to produce these metrics. In this way, the Oracle Database Solution implements the equivalent of many of the system monitoring scripts that come bundled with the Oracle installation.

The Oracle Database solution templates provide comprehensive Oracle database monitoring without requiring the SiteScope user or the IT organization to be an expert on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.



---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the Oracle Database solution template. Contact your HP Sales representative for more information about Solution licensing.
  - ▶ An in-depth description of the Oracle Database Solution is available in the SiteScope Oracle Database Best Practices document. This document is part of the SiteScope installation, and can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_Oracle_Database_Best_Practices.pdf`. This is a password protected document. The password is provided along with the Oracle Database Solution license key from HP.
- 

## Solution Template Monitors

The Oracle Database solution template deploys monitors that target the following aspects of Oracle performance and health:

- ▶ **General System Statistics.** The most important V\$SYSSTAT statistics are monitored by default in the monitors deployed by the Oracle Database Solution. Where applicable, these metrics are combined to calculate deltas and rates on a per-second or per-transaction basis. When monitoring the important metrics from the V\$ tables in the database, the Oracle Database Solution is a replacement for manually generated SQL scripts.
- ▶ **Oracle Logs.** Important Oracle log files are monitored for ORA- errors. Users may customize these monitors to look for specific text in a log file, depending on their database configuration.
- ▶ **Diagnosing Database Problems.** In addition to the deployed monitors, Oracle Solution offers several tools that can be used to gain diagnostic information about a database. Resource-intensive SQL statements, shared server process contention, and the number of sessions waiting for specific events are all examples of the diagnostic data that these tools can provide.

## **Deploy Oracle Database Solution Templates**

This task describes the steps involved in configuring the server environment and entering variables for the Oracle Database solution template.

This task includes the following steps:

- “Prerequisites” on page 1762
- “Configure the Oracle Database Server Environment” on page 1762
- “Deploy the Solution Template” on page 1762
- “Enter Deployment Values for the Solution Template” on page 1762

### **1 Prerequisites**

You must have CREATE SESSION system privileges to successfully deploy the Oracle Database 9i and 10g solution template.

### **2 Configure the Oracle Database Server Environment**

Follow the usage guidelines and perform the configuration requirements involving the server environment. For details on this topic, see “Oracle Database Solution Template Usage Guidelines” on page 1763.

### **3 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **4 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the Oracle Database solution template. For details on the user interface, see “Oracle Solution Template User Interface” on page 1766.

## Oracle Database Solution Template Usage Guidelines

Before configuring the Oracle Database Solution for deployment, consult the documentation for the Database Counter Monitor (see “Database Counter Monitor Overview” on page 467) and the Log File Monitor (see “Log File Monitor Settings” on page 600) for information about some of the prerequisites and parameters required by the solution template. For example, you find more information on installing the Oracle JDBC driver needed to communicate with the database and the format of the log file path parameter.

## Oracle Database Solution Template Tools

The Oracle Database solution template deploys several tools that you can use to gather diagnostic information about an Oracle database. These tools are deployed to the same group as the monitors that are deployed by the solution template. They are displayed in much the same way as monitors but they are set as disabled. These tools are identified by the bold text **Solution Tool** in the **Status** field of the group content table. Although the Solution tools are listed in the monitor table, they are not monitor instances. They do not run automatically, do not display a status based on action results, nor do they trigger alerts. They are preconfigured actions that make use of a SiteScope Diagnostic Tool to check certain statistics from the Oracle database that may indicate a performance problem.

When the user clicks on one of these Solution Tools, SiteScope makes a custom SQL query to the database by using the Database Connection Test tool. The results of the query are found in a table at the bottom of the page. From this page, the tool may be run as many times as necessary by clicking the Connect and Execute Query button. Bear in mind that some tools may incur substantial overhead on the database, so executing them in quick succession is not recommended.

## List of Oracle Database Solution Tools

The following describes tools deployed as part of the Oracle Database Solution:

Oracle Solution Tool Name	Description and Usage Guidelines
Top Ten SQL Statements in Logical IOs Per Row	<p>This tool performs a query which is designed to locate the most resource-intensive SQL statements being run in the database. The V\$SQL table is queried for the ten SQL statements which are performing the most logical IOs per row are displayed in a table.</p> <p>The statement IDs of these ten statements are displayed in a table, along with some additional resource-usage data for each statement.</p> <p>This additional data includes:</p> <ul style="list-style-type: none"> <li>▶ <b>Physical IO Blocks.</b> The number of disk reads performed on behalf of the statement.</li> <li>▶ <b>Logical IOs.</b> The number of buffer gets performed on behalf of the statement.</li> <li>▶ <b>Rows Processed.</b> The number of rows processed when executing the statement.</li> <li>▶ <b>Logical IOs Per Row.</b> The number of buffer gets performed per row that was processed when executing the statement.</li> <li>▶ <b>Runs.</b> The number of executions of the statement.</li> <li>▶ <b>Logical IOs Per Run.</b> The number of buffer gets per statement execution.</li> </ul> <p><b>Note:</b> The action performed can have a significant affect on database resources and should not be run frequently.</p>
Number of Sessions Waiting Per Event	<p>This tool can be used in troubleshooting stuck sessions. When several sessions become unresponsive, this tool can determine whether the stuck sessions are all waiting on the same event. The tool action displays a table containing the number of sessions waiting on specific events.</p>

Oracle Solution Tool Name	Description and Usage Guidelines
Shared Server Process Contention (Common Queue Average Wait Time)	This tool calculates the average wait time of the shared server message queue (the Common Queue as recorded in V\$QUEUE). A high average wait time may indicate contention between shared server processes.

Use the following steps to run the Oracle Database Solution tools.

**To run an Oracle Database Solution tool:**

- 1** Click the group name for the group where the Oracle Solution monitors are deployed. The Group Detail page opens.
- 2** Find the Solution Tool for the action that you want to run. See the **Name** column for the Solution Tool for a description of the action performed by that tool.
- 3** Click the **Tools** link to the right of the tool **Name** to run the action. The Database Connection Test page opens. From this page, the tool may be run as many times as necessary by clicking the **Connect and Execute Query** button.

---

**Note:** Some Solution Tools may create significant overhead on the database depending on the query. Therefore, we do not recommend that you run the tools in quick succession.

---

The upper portion of the Database Connection Test page displays the database connection parameters used for the test. The results of the tool query are found in a table near the bottom of the page. Review the results based on the Description and Usage Guidelines for that tool.

## Oracle Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the Oracle solution template.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select <b>Oracle Database 9i and 10g</b>.</p>
<b>Important Information</b>	You must have CREATE SESSION system privileges to successfully deploy the Oracle Database 9i and 10g solution template.
<b>Included in Tasks</b>	"Deploy a SiteScope Solution Template – Workflow" on page 1669
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ "Oracle Database Solution Template" on page 1759</li> <li>➤ "Template Tree" on page 84</li> </ul>

### Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>DatabaseConnection URL</b>	<p>The connection URL to the database you want to connect to. The syntax is jdbc:oracle:thin:@&lt;server name or IP address&gt;:&lt;database server port&gt;;sid=&lt;sid&gt;.</p> <p><b>Example:</b> To connect to the ORCL database on a machine using port 1521 you would use: jdbc:oracle:thin:@206.168.191.19:1521:ORCL.</p> <p><b>Note:</b> The colon (;) and (@) symbols must be included as shown.</p>
<b>DatabaseDriver</b>	<p>The name of the JDBC driver to be used by this monitor. Each driver supports a specific connection URL pattern, so it must match the URL entered in <b>Database Connection URL</b>.</p>

GUI Element	Description
<b>OracleAlertLogPath</b>	The full path to the Oracle alert log. For Windows machines, this should be the full UNC path. Enter the full path to the Oracle alert log. Consult your database administrator or the Oracle documentation for information about how to access this file.
<b>OracleListenerLog Path</b>	The full path to the Oracle listener log. For Windows machines, this should be the full UNC path. Consult your database administrator or the Oracle documentation for information about how to access this file.
<b>DatabaseUserName</b>	The user name that SiteScope should use to connect to the database.
<b>DATABASEPASSWORD</b>	The password for the user name that SiteScope should use to connect to the database.
<b>Log File Encoding</b>	<p>If the file content to be monitored uses an encoding that is different than the encoding used on server where SiteScope is running, enter the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the target file. This enables SiteScope to match and display the encoded file content correctly.</p> <p><b>Examples:</b> Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.</p>
<b>SERVER_LIST</b>	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a connection profile, see “Configure SiteScope to Monitor a Remote Microsoft Windows Server” on page 1277 and “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285.

GUI Element	Description
<b>Silent deployment</b>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to &lt;SiteScope root directory&gt;\logs\silent_deployment.log.</p> <p><b>Default value:</b> Not selected</p>
<b>Verify monitor properties with remote server</b>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>



---

## SAP Solution Templates

This chapter includes the main concepts, tasks, and reference information for the SAP solution templates.

**This chapter includes:**

**Concepts**

- ▶ SAP Solution Overview on page 1770

**Tasks**

- ▶ Deploy the SAP Solution Template on page 1771

**Reference**

- ▶ SAP Solution Template Configuration Requirements on page 1772
- ▶ SAP Solution Template User Interface on page 1773

## SAP Solution Overview

The SAP solution includes solution templates for the monitoring the following key SAP components:

- SAP CCMS
- SAP Java Web Application Server

The SAP Solution uses two solution templates which you use to deploy a collection of monitors configured with metrics to report on availability and performance. These monitoring configurations have been researched using best practice data and expertise from various sources.

The SAP solution templates provide comprehensive SAP monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

---

**Note:** You must have the applicable SiteScope option license to use the SAP R/3 Application Server and SAP NetWeaver Application Server solution templates. Contact your HP sales representative for more information about licensing for solution templates.

---

You use the SAP R/3 Application Server solution template to deploy monitoring for SAP R/3 systems. You use the SAP NetWeaver Application Server template to monitor the SAP Java Web Application server if this component is deployed in the IT environment.

## Deploy the SAP Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the SAP solution template.

This task includes the following steps:

- “Configure the SAP Server Environment” on page 1771
- “Deploy the Solution Template” on page 1771
- “Enter Deployment Values for the Solution Template” on page 1771

### **1 Configure the SAP Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “SAP Solution Template Configuration Requirements” on page 1772.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the SAP solution template. For details on the user interface, see “SAP Solution Template User Interface” on page 1773.

## **SAP Solution Template Configuration Requirements**

### **SAP R/3 Application Server Solution Template**

The SiteScope SAP R/3 Application Server solution template provides the tools you use to monitor the availability, usage statistics, and server performance statistics for SAP R/3 systems. This solution template deploys a set of monitors that test the health, availability, and performance of SAP R/3 servers.

Before you can use the SAP R/3 Application Server solution template, there are a number of configuration requirements involving the server environment. The following lists an overview of these requirements:

- ▶ SAP Java Connector libraries should be copied to the required SiteScope folders.
- ▶ You must know the user name and password that SiteScope must use to log into the SAP R/3 server.

For more information on system and configuration requirements, see “SAP CCMS Monitor Overview” on page 788. This monitor is deployed as part of the SAP R/3 solution template.

### **SAP NetWeaver Application Server Solution Template**

The SiteScope SAP NetWeaver Application Server solution enables you to monitor the availability and server statistics for SAP Java Web application server clusters.

This solution template deploys a monitor that tests the health, availability, and performance of SAP Java Web application servers. You can use this solution template to deploy monitors for server-wide resources and metrics.

Before you can use the SAP NetWeaver Application Server solution template, there are a number of configuration requirements involving the server environment. The following lists an overview of these requirements:

- ▶ SAP Java Web application server libraries must be copied to the required SiteScope folders.
- ▶ You must know the user name and password that SiteScope must use to log into the SAP Java Web application server.

For more information on system and configuration requirements, see “SAP Java Web Application Server Monitor Overview” on page 808. This monitor is deployed as part of the SAP NetWeaver Application Server solution template.

## SAP Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the SAP solution templates for monitoring key components on SAP CCMS and SAP Java Web Application Servers.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select the required SAP solution template.</p>
<b>Included in Tasks</b>	<p>“Deploy a SiteScope Solution Template – Workflow” on page 1669</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SAP Solution Templates” on page 1769</li> <li>▶ “Template Tree” on page 84</li> </ul>

## SAP R/3 Application Server

The Main Settings include the following elements:

GUI Element	Description
<b>CLIENT_NUMBER</b>	The Client to use for connecting to SAP.
<b>Password</b>	The password required to connect to the SAP server.
<b>USER_NAME</b>	The user name required to connect to the SAP server.
<b>SYSTEM_NUMBER</b>	The System number for the SAP server.
<b>APPLICATION_SERVER</b>	The address of the SAP server you want to monitor.
<b>Silent deployment</b>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to &lt;SiteScope root directory&gt;\logs\silent_deployment.log.</p> <p><b>Default value:</b> Not selected</p>
<b>Verify monitor properties with remote server</b>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>

## SAP NetWeaver Application Server

The Main Settings include the following elements:

GUI Element	Description
<b>TARGET_SERVER_NAME</b>	The address of the SAP Java Web Application Server you want to monitor.
<b>USER_NAME</b>	The user name required to connect to the SAP Java Web Application Server.
<b>PORT</b>	The port for the SAP Java Web Application Server.
<b>Password</b>	The password required to connect to the SAP Java Web Application Server.
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <SiteScope root directory>\logs\silent_deployment.log. <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected





# 147

---

## Siebel Solution Templates

This chapter includes the main concepts, tasks, and reference information for the Siebel solution templates.

### **This chapter includes:**

#### **Concepts**

- ▶ Siebel Solution Overview on page 1778

#### **Tasks**

- ▶ Deploy the Siebel Solution Template on page 1780

#### **Reference**

- ▶ Siebel Solution Configuration Requirements on page 1781
- ▶ Siebel Solution Template User Interface on page 1782

## Siebel Solution Overview

The SiteScope Siebel solution templates provide efficient and thorough monitoring of performance, availability, and usage statistics for Siebel Application, Gateway, and Web servers installed on Microsoft Windows and UNIX operating systems. There are separate solution templates for servers installed on UNIX and Windows platforms.

The primary solution template for Siebel is the Siebel Application Server template. You use this template to deploy monitoring for the core of the Siebel application. You use the Siebel Gateway Server and Siebel Web Server templates if these optional components are deployed in the IT environment.

The Siebel solution templates provide comprehensive Siebel monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy various performance monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the Siebel solution templates. Contact your HP sales representative for more information about Solution licensing.
  - ▶ An in-depth description of the Siebel Solution is available in the SiteScope Siebel Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope\_Siebel\_Best\_Practices.pdf**. This is a password protected document. The password is provided along with the Siebel Solution license key from HP.
-

## Solution Template Monitors

The Siebel Solution includes solution templates for monitoring the following key Siebel components:

- ▶ **Siebel Application Server for UNIX/Windows.** The SiteScope Siebel Application Server Solutions allow you to monitor the availability, usage statistics, and server performance statistics for Siebel Application servers installed on Windows and UNIX platforms. These solution templates deploy a set of monitors that test the health, availability, and performance of Siebel 6.x, 7.x, and 8.x application servers.
- ▶ **Siebel Gateway Server for UNIX/Windows.** The SiteScope Siebel Gateway Server Solutions allow you to monitor the availability and server statistics for Siebel Gateway servers installed on Windows and UNIX platforms. These solution templates deploy a set of monitors that test the health, availability, and performance of Siebel Gateway Servers. You can use these solution templates to deploy monitors for server-wide resources and metrics.
- ▶ **Siebel Web Server for UNIX/Windows.** The SiteScope Siebel Web Server Solutions allow you to monitor the availability and server statistics for Siebel Web servers installed on Windows and UNIX platforms. These solution templates deploy a set of monitors that test the health, availability, and performance of Siebel Web Servers.

## **Deploy the Siebel Solution Template**

This task describes the steps involved in configuring the server environment and entering variables for the Siebel Solution Template.

This task includes the following steps:

- “Configure the Siebel Server Environment” on page 1780
- “Deploy the Solution Template” on page 1780
- “Enter Deployment Values for the Solution Template” on page 1780

### **1 Configure the Siebel Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “Siebel Solution Configuration Requirements” on page 1781.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the Siebel solution template. For details on the user interface, see “Siebel Solution Template User Interface” on page 1782.

## Siebel Solution Configuration Requirements

Before you can use the Siebel Application or Web Server Solution, there are a number of configuration requirements involving the server environment.

This section includes the following topics:

- “Siebel Application Server Solution Template” on page 1781
- “Siebel Web Server Solution Template” on page 1782

### **Siebel Application Server Solution Template**

- The Siebel Server Manager client must be installed only on a Windows machine where SiteScope is running or that is accessible to the SiteScope machine (even if the Siebel application server is installed on UNIX). There are several options for how you can do this. See the documentation for the Siebel Server Manager Monitor for more information.
- You must know the install path for the Server Manager client to be able to setup Siebel Server Manager monitors in SiteScope. If the client is installed on the machine where SiteScope is running, this is the path on that machine. If the client is installed on a remote machine, you must know the fully qualified path to the client executable relative to that machine.
- You must know the name of the Siebel applications that are available in your network. For example, call center, sales, and so on.
- You must know the Siebel database machine name, user name, password, connection URL, and Database Driver.
- You must know the user and password that SiteScope uses for logging into the Siebel server. This user must be granted Siebel Administrator responsibility on the Siebel server.
- You must make sure that the following Siebel server component groups are enabled:
  - Siebel Call Center (CallCenter)
  - Siebel Remote (Remote)
  - System Management (System)
  - Auxiliary System Management (SystemAux) - Siebel 8.x only

- ▶ You need to know a significant list of Siebel system component names and their corresponding aliases. For a listing of component names and aliases, see “Siebel Solution Template User Interface” on page 1782.

For more information on system and configuration requirements, see the sections on the “Siebel Web Server Monitor Overview” on page 873 and “Database Query Monitor Overview” on page 477. These monitor types that are deployed as part of the Siebel Application Server solution template.

### Siebel Web Server Solution Template

- ▶ SiteScope server must be able to connect to the machine where the Siebel Web Server is running.
- ▶ Siebel Web Server Solution is designed for use with Siebel running on Microsoft Windows platforms.
- ▶ Template assumes that the Siebel Web Server is running on Microsoft Internet Information Server (IIS).

## Siebel Solution Template User Interface

<p><b>Description</b></p>	<p>Enables you to deploy the Siebel solution templates for monitoring the Siebel 6.x, 7.x, and 8.x Application Server, Siebel Gateway Server, and Siebel Web Server on Windows and UNIX platforms.</p> <p>Use this page to add the server monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select the required Siebel solution template.</p>
<p><b>Included in Tasks</b></p>	<p>“Deploy a SiteScope Solution Template – Workflow” on page 1669</p>
<p><b>Useful Links</b></p>	<ul style="list-style-type: none"> <li>▶ “Siebel Solution Templates” on page 1777</li> <li>▶ “Template Tree” on page 84</li> </ul>

## Siebel Application Server

The Main Settings include the following elements for monitoring Siebel Application Server 6.x, 7.x, and 8.x on Windows and UNIX environments:

GUI Element (A-Z)	Description
<b>Application</b>	The Siebel Application Server machine name.
<b>CG_Auxiliary_System_Management_Alias</b> (Siebel 8.x only)	The Siebel Auxiliary System Management component group alias.
<b>CG_Auxiliary_System_Management_Name</b> (Siebel 8.x only)	The Siebel Auxiliary System Management component group name.
<b>CG_Callcenter_Alias</b>	The Siebel CallCenter component group alias.
<b>CG_Callcenter_Name</b>	The Siebel CallCenter component group name.
<b>CG_System_Management_Alias</b>	The Siebel System Management component group alias.
<b>CG_System_Management_Name</b>	The Siebel System Management component group name.
<b>CP_Callcenter_Alias</b>	The Siebel CallCenter component alias.
<b>CP_Callcenter_Name</b>	The Siebel CallCenter component name.
<b>CP_Client_Administration_Alias</b> (Siebel 6.x-7.x only)	The Siebel Client Administration component alias.
<b>CP_Client_Administration_Name</b> (Siebel 6.x-7.x only)	The Siebel Client Administration component name.
<b>CP_eService_Alias</b>	The Siebel eService component alias.
<b>CP_eService_Name</b>	The Siebel eService component name.
<b>CP_File_System_Manager_Alias</b>	The Siebel File System Manager component alias.

GUI Element (A-Z)	Description
<b>CP_File_System_Manager_Name</b>	The Siebel File System Manager component name.
<b>CP_Server_Manager_Alias</b>	The Siebel Server Manager component alias.
<b>CP_Server_Manager_Name</b>	The Siebel Server Manager component name.
<b>CP_Server_Request_Broker_Alias</b>	The Siebel Server Request Broker component alias.
<b>CP_Server_Request_Broker_Name</b>	The Siebel Server Request Broker component name.
<b>CP_Server_Request_Processor_Alias</b>	The Siebel Server Request Broker component alias.
<b>CP_Server_Request_Processor_Name</b>	The Siebel Server Request Processor component name.
<b>Database_Connection_URL</b>	<p>The URL to the database connection.</p> <p><b>Example:</b> If the ODBC connection is called <code>test</code>, the URL is <code>jdbc:odbc:test</code>.</p> <p>Enter the connection URL to the database you want to connect to. The syntax is <code>jdbc:oracle:thin:@&lt;server name or IP address&gt;:&lt;database server port&gt;;sid=&lt;sid&gt;</code>.</p> <p><b>Example:</b> To connect to the ORCL database on a machine using port 1521 use: <code>jdbc:oracle:thin:@206.168.191.19:1521:ORCL</code>.</p> <p><b>Note:</b> The colon and <code>@</code> symbols must be included as shown.</p>
<b>Database_Driver</b>	The driver used to connect to the database.
<b>Database_PASSWORD</b>	The password for the user name used to access the Siebel database.
<b>Database_Username</b>	The user name SiteScope should use to access the Siebel database.
<b>Enterprise</b>	The Siebel Enterprise server name.



GUI Element (A-Z)	Description
Gateway	The name of the Siebel Gateway server machine.
PASSWORD	The password for the Siebel Client.
SERVER_LIST	Select the server where the Siebel Application Server is running.
Server_Logical_Instance_Name	The Siebel server logical name.
Server_Manager_Path	The local path to the Siebel server manager client. <b>Example:</b> D:\sea703\client\bin.
Siebel_Database_Machine_Name	The Siebel database machine name.
Siebel_Disk	The disk drive name where Siebel is installed.
Siebel_Root_Dir	The path of the shared Siebel root directory. <b>Example:</b> The shared root directory for a Siebel 7.5.2 server would be: sea752.
Username	The Siebel Client user name.
Silent deployment	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <SiteScope root directory>\logs\silent_deployment.log. <b>Default value:</b> Not selected
Verify monitor properties with remote server	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected

## Siebel Gateway Server

The Main Settings include the following elements:

GUI Element	Description
<b>Siebel_Root_Dir</b>	The path to the Siebel root directory. This directory should contain at least an Admin Console installation.
<b>Siebel_Disk</b>	The disk drive where the Siebel gateway server is running.
<b>Siebel_Logical_Instance_Name</b>	The Siebel server logical name value (for UNIX only).
<b>SERVER_LIST</b>	The name of the server where the Siebel Gateway Server is running. Do not type backslashes (\\), which indicates a UNC path as part of the name of the server.
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <SiteScope root directory>\logs\silent_deployment.log. <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected

## Siebel Web Server

The Main Settings include the following elements:

GUI Element	Description
<b>Application</b>	The Siebel application to monitor. <b>Example:</b> callcenter_enu. Consult with your Siebel administrator for information about names of the installed Siebel applications.
<b>Siebel_Disk</b>	The disk drive name or drive letter where the Siebel Web server is installed.
<b>Siebel_Root_Dir</b>	The name of the shared Siebel root directory. <b>Example:</b> Siebel root directory on Windows: sea752.
<b>Siebel_Logical_Instance_Name</b>	The Siebel server logical name value (for UNIX only).
<b>Username</b>	The Siebel Client user name needed to log into the Siebel Web server.
<b>Password</b>	The Siebel Client password needed to log into the Siebel Web server.
<b>SERVER_LIST</b>	Select the Siebel Web server machine name. Use the choose server to view the server selection page. Use the Server drop-down menu to select the server where the Siebel Web server is running.

GUI Element	Description
<p><b>Silent deployment</b></p>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to &lt;SiteScope root directory&gt;\logs\silent_deployment.log.</p> <p><b>Default value:</b> Not selected</p>
<p><b>Verify monitor properties with remote server</b></p>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>

# 148

---

## Solaris Host Solution Templates

This chapter includes the main concepts, tasks, and reference information for the Solaris Host solution template.

### **This chapter includes:**

#### Concepts

- ▶ Solaris Host Solution Overview on page 1789

#### Tasks

- ▶ Deploy the Solaris Host Solution Template on page 1791

#### Reference

- ▶ Solaris Host Solution Configuration Requirements on page 1792
- ▶ Solaris Host Solution Template User Interface on page 1792

### **Solaris Host Solution Overview**

The Solaris Host solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the Solaris host. The template supports the versions of Solaris that are supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can create a Server-Centric report which displays data from three different metrics about the server being monitored. We recommend that you use solution templates when creating the UNIX Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric report, see “Generating a Server-Centric Report” on page 1881.

The Solaris Host solution template provides comprehensive Solaris operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the Solaris Host solution template. Contact your HP sales representative for more information about Solution licensing.
  - ▶ An in-depth description of the Solaris Host Solution settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at <**SiteScope root directory**>\sidsdocs\pdfs\**SiteScope\_OS\_Best\_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.
- 

### **Solution Template Monitors**

The Solaris Host solution template deploys monitors that target the following aspects of Solaris performance and health:

- ▶ CPU status and utilization details
- ▶ Memory status and utilization details
- ▶ File system status and utilization details

## Deploy the Solaris Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Solaris Host solution template.

---

**Note:** The Solaris Host solution template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Server-Centric Report support.

---

This task includes the following steps:

- “Configure the Solaris Server Environment” on page 1791
- “Deploy the Solution Template” on page 1791
- “Enter Deployment Values for the Solution Template” on page 1791

### **1 Configure the Solaris Server Environment**

Perform the configuration requirements involving the server environment. For details on this topic, see “Solaris Host Solution Configuration Requirements” on page 1792.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the Solaris Host solution template. For details on the user interface, see “Solaris Host Solution Template User Interface” on page 1792.

## Solaris Host Solution Configuration Requirements

Before you can use the Solaris Host solution template, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the target Solaris host.
- The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test (**Remote Servers > UNIX Remote Servers**). For details, see “New/Edit UNIX Remote Servers Dialog Box” on page 1299.
- The SiteScope server itself can also be monitoring if it runs a supported Solaris operating system.
- The template supports the Solaris versions supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

## Solaris Host Solution Template User Interface

<b>Description</b>	Enables you to deploy the Solaris solution template. Use this page to add the server monitor or edit the monitor's properties. <b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b> , and select <b>Solaris Host</b> .
<b>Included in Tasks</b>	“Deploy a SiteScope Solution Template – Workflow” on page 1669
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Solaris Host Solution Templates” on page 1789</li> <li>➤ “Template Tree” on page 84</li> </ul>



## Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>SERVER_LIST</b>	Choose the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a UNIX connection profile, see “Configure SiteScope to Monitor a Remote UNIX Server” on page 1285.
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <b>&lt;SiteScope root directory&gt;\logs\silent_deployment.log</b> . <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected



# 149

---

## WebLogic Solution Template

This chapter includes the main concepts, tasks, and reference information for the WebLogic solution templates.

### **This chapter includes:**

#### **Concepts**

- ▶ WebLogic Solution Overview on page 1796

#### **Tasks**

- ▶ Deploy the WebLogic Solution Template on page 1798

#### **Reference**

- ▶ WebLogic Solution Usage Guidelines on page 1799
- ▶ Selecting WebLogic Modules for Monitoring on page 1799
- ▶ WebLogic Solution Template User Interface on page 1801

## WebLogic Solution Overview

The WebLogic solution template is a template that you can use to deploy a collection of WebLogic Monitors configured with default metrics. The monitors test the health, availability, and performance of a WebLogic Application Server and its deployed applications and components. The deployed monitors check server-wide statistics such as memory usage, as well as metrics specific to individual J2EE components, such as the number of activates and passivates of a particular EJB.

Use the WebLogic Solution to monitor statistics from WebLogic 6.x, 7.x, 8.x, 9.x, and 10.x servers. This solution automatically creates several groups by default which monitor important application server metrics, but it also provides a user interface that allows you to select all or some of the individual components that are available for monitoring.

The WebLogic Solution monitor deployment process is highly customizable in that it allows the user to select the specific J2EE components on an application server which SiteScope should actively monitor.

The WebLogic solution templates provide comprehensive WebLogic monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

---

### Note:

- ▶ You must have the applicable SiteScope option license to use the WebLogic solution template. Contact your HP sales representative for more information about Solution licensing.
  - ▶ An in-depth description of the WebLogic Solution is available in the SiteScope WebLogic Best Practices document. This document is part of the SiteScope installation, and can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_WebLogic_Best_Practices.pdf`. This is a password protected document. The password is provided along with the WebLogic Solution license key from HP.
-

## Solution Template Monitors

The WebLogic solution template deploys monitors that target the following aspects of WebLogic performance and health:

- ▶ **Server Performance Statistics.** This category refers to a collection of server-wide resources that are exposed through the management interface of a WebLogic Application Server.
- ▶ **Application Performance Statistics.** Metrics for all of your deployed applications, EJBs, web applications, and servlets are available for monitoring through the WebLogic Solution. The user is responsible for selecting which of these J2EE components he would like to have monitors automatically deployed for. A set of metrics based on WebLogic best practices are monitored for each selected J2EE component.
- ▶ **WebLogic Solution Metrics.** For the list of components that can be monitored, see the SiteScope WebLogic Best Practices document.

## **Deploy the WebLogic Solution Template**

This task describes the steps involved in configuring the server environment and entering variables for the WebLogic solution template.

This task includes the following steps:

- “Configure the WebLogic Server Environment” on page 1798
- “Deploy the Solution Template” on page 1798
- “Enter Deployment Values for the Solution Template” on page 1798

### **1 Configure the WebLogic Server Environment**

Follow the usage guidelines and perform the configuration requirements involving the server environment. For details on this topic, see “WebLogic Solution Usage Guidelines” on page 1799.

### **2 Deploy the Solution Template**

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### **3 Enter Deployment Values for the Solution Template**

Complete the items on the Deployment Values page for the WebLogic solution template. For details on the user interface, see “WebLogic Solution Template User Interface” on page 1801.

## **WebLogic Solution Usage Guidelines**

The WebLogic solution template deploys a WebLogic Application Server Monitor for each module that is selected from the user interface. This monitor uses the Java JMX interface to access Runtime MBeans on the WebLogic server. An MBean is a container that holds the performance metrics. You may need to set certain permissions on the WebLogic server for SiteScope to be able to monitor MBeans. For an overview on configuring access to WebLogic servers for SiteScope monitors, see “WebSphere Application Server Monitor Overview” on page 1072.

## **Selecting WebLogic Modules for Monitoring**

The WebLogic Solution presents a hierarchical list from which the user can select the modules to deploy WebLogic Monitors against. This list is broken down into two main sections:

- per-server resources
- J2EE components organized by application

Some of the modules in these categories are automatically selected by default because they represent critical components in the system (for example, the JVM statistics for the application server). The remainder of the modules are not automatically selected. This allows the user to customize the deployment of this solution to focus on one application, a particular type of EJB, a set of servlets and web applications, or some other aspect of the application server.

For the most part, the organization of this list of modules is intuitive. The hierarchy of applications, EJBs, web applications, and servlets is very similar to the organization of these entities in the WebLogic Administration Console. In almost every case, selecting a module causes a monitor with all relevant metrics to be deployed against that part of the WebLogic server. However, when selecting EJBs to monitor, you notice that they are broken down according to three types of metrics: Pool, Transaction, and Cache. The reason for this is twofold: (1) it is more useful to be able to monitor one aspect of a particular EJB instead per WebLogic Monitor for purposes of alerting and organization, and (2) not all three of these types of metrics are available for all EJBs.

Below is a brief description of the metrics that are monitored for each type of EJB monitoring:

- **Per-EJB Transaction Statistics.** This category of EJB monitor contains metrics related to transactions made for the EJB. These metrics include the number of transactions rolled back, the number of transactions that timed out, and the number of transactions that were successfully committed.
- **Per-EJB Pool Statistics.** This category of EJB monitor contains metrics related to the pool for the EJB. When the user selects an EJB under this heading, many useful metrics are monitored, including the number of times an attempt to get a bean instance from the pool failed, the number of current available instances in the pool, the number of threads currently waiting for an instance, and the number of times a bean instance was destroyed due to a non-application exception.
- **Per-EJB Cache Statistics.** The cache statistics include any metrics relating to the caching of the particular EJB. Metrics like the number of cache hits and misses, and the number of activates and passivates of the EJB are monitored when an EJB under this heading is selected for monitoring.

When you have finished making your module selections in the popup window, scroll to the bottom of the Module Selection window and click the **Select Modules** button. This updates the main browser window with a list of the modules you selected. You can then review your selections and remove any modules that you don't want a monitor to be created for.

When you are satisfied with the list of selected modules in the main browser window, click **Submit**.



## WebLogic Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the WebLogic solution template for monitoring BEA WebLogic 6.x, 7.x, 8.x, 9.x, and 10.x application servers.</p> <p>Use this page to add the server monitor or edit the monitor's properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select the required WebLogic solution template.</p>
<b>Included in Tasks</b>	“Deploy a SiteScope Solution Template – Workflow” on page 1669
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “WebLogic Solution Template” on page 1795</li> <li>▶ “Template Tree” on page 84</li> </ul>

### WebLogic 9.x-10.x

The Main Settings include the following elements:

GUI Element	Description
<b>WEBLOGIC_URL</b>	<p>The URL for the WebLogic 9.x or 10.x application server. The default is:</p> <pre>service:jmx:rmi:///jndi/iiop://&lt;local host&gt;:7001/weblogic.management.mbeanservers.runtime</pre> <p>where &lt;local host&gt; is the name of the machine running WebLogic Application Server 9.x or 10.x.</p>
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.

GUI Element	Description
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <b>&lt;SiteScope root directory&gt;\logs\silent_deployment.log</b> . <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected

### WebLogic 6.x, 7.x, 8.x

The Main Settings include the following elements:

GUI Element	Description
<b>WEBLOGIC_PORT</b>	The port number that the WebLogic server is responding on. <b>Default value:</b> 7001
<b>WEBLOGIC_PASSWORD</b>	The password required to log into the WebLogic server.
<b>WEBLOGIC_USERNAME</b>	The user name required to log into the WebLogic server.
<b>WEBLOGIC_SERVER</b>	The name or address of the server where WebLogic is running.

GUI Element	Description
<b>WEBLOGIC_TIMEOUT</b>	The number of seconds to wait for a data request to arrive at the WebLogic server. <b>Default value:</b> 180
<b>WEBLOGIC_JAR_FILE</b>	The absolute path to the weblogic.jar file on the SiteScope machine. This file must be installed on the SiteScope server and can be downloaded from the WebLogic server. <b>Example:</b> c:\bea\weblogic7\ebcc\lib\ext\weblogic.jar.
<b>Counters</b>	The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.
<b>Silent deployment</b>	Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <SiteScope root directory>\logs\silent_deployment.log. <b>Default value:</b> Not selected
<b>Verify monitor properties with remote server</b>	Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. <b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection. <b>Default value:</b> Selected



# 150

---

## WebSphere Solution Template

This chapter includes the main concepts, tasks, and reference information for the WebSphere solution templates.

### **This chapter includes:**

#### Concepts

- ▶ WebSphere Solution Overview on page 1805

#### Tasks

- ▶ Deploy the WebSphere Solution Template on page 1807

#### Reference

- ▶ WebSphere Solution Template User Interface on page 1808

### **WebSphere Solution Overview**

The WebSphere solution template is a template that you can use to deploy a collection of WebSphere Monitors configured with default metrics. The monitors test the availability, server statistics, and deployed J2EE components for IBM WebSphere Application Server 5.x and 6.x. You can use this solution template to deploy monitors for server-wide resources and metrics (for example, thread pool and JVM metrics). You can also create monitors for the deployed EJBs, Web Applications, and Servlets using this solution template.

The WebSphere Solution monitor deployment process is highly customizable in that it allows the user to select the specific J2EE components on an application server which SiteScope should actively monitor.

The WebSphere solution templates provide comprehensive WebSphere monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

---

**Note:**

- ▶ You must have the applicable SiteScope option license to use the WebSphere solution templates. Contact your HP Sales representative for more information about Solution licensing.
  - ▶ An in-depth description of the WebSphere Solution is available in the SiteScope WebSphere Best Practices document. This document is part of the SiteScope installation, and can be found at `<SiteScope root directory>\sisdocs\pdfs\SiteScope_WebSphere_Best_Practices.pdf`. This is a password protected document. The password is provided along with the WebSphere Solution license key from HP.
- 

## **Solution Template Monitors**

The WebSphere solution template deploys monitors that target the following aspects of WebSphere performance and health:

- ▶ **Server Performance Statistics.** This category refers to a collection of server-wide resources that are exposed through the management interface of a WebSphere Application Server.
- ▶ **Application Performance Statistics.** Metrics for all of your deployed applications, EJBs, web applications, and servlets are available for monitoring through the WebSphere Solution. The user is responsible for selecting which of these J2EE components he would like to have monitors automatically deployed for. A set of metrics based on WebSphere best practices are monitored for each selected J2EE component.
- ▶ **WebSphere Application Server Solution Metrics.** For the list of components that can be monitored, see the SiteScope WebSphere Best Practices document.

## Deploy the WebSphere Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the WebSphere solution template.

This task includes the following steps:

- “Configure the WebSphere Server Environment” on page 1807
- “Deploy the Solution Template” on page 1807
- “Enter Deployment Values for the Solution Template” on page 1808

### 1 Configure the WebSphere Server Environment

Perform the configuration requirements involving the server environment. For an overview of these requirements, see “WebSphere Application Server Monitor Overview” on page 1072.

---

**Note:** By default, the WebSphere 6.x Application Server solution template uses the internal JVM mechanism. Accordingly, when using this solution template you should configure the monitoring environment to use internal Java. For details, see “Configure the WebSphere 6.0x Server Environment Using Internal Java” on page 1079 and “Configure the WebSphere 6.1x Server Environment Using Internal Java” on page 1085.

---

### 2 Deploy the Solution Template

For a detailed overview of the steps involved in deploying a solution template, see “Deploy a SiteScope Solution Template – Workflow” on page 1669.

### 3 Enter Deployment Values for the Solution Template

Complete the items on the Deployment Values page for the WebSphere solution template. For details on the user interface, see “WebSphere Solution Template User Interface” on page 1808.

## WebSphere Solution Template User Interface

<b>Description</b>	<p>Enables you to deploy the WebSphere solution template for monitoring IBM WebSphere Application Servers 5.x and 6.x.</p> <p>Use this page to add the server monitor or edit the monitor’s properties.</p> <p><b>To access:</b> Open the <b>Templates</b> context. In the template tree, expand <b>Solution Templates</b>, and select the required WebSphere solution template.</p>
<b>Included in Tasks</b>	“Deploy a SiteScope Solution Template – Workflow” on page 1669
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “WebSphere Solution Template” on page 1805</li> <li>➤ “Template Tree” on page 84</li> </ul>

### Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>WEBSHERE_CLIENT_PROPERTIES_FILE</b>	<p>The client properties file.</p> <p><b>Default value:</b> /properties/soap.client.props</p>
<b>WEBSHERE_PORT</b>	<p>The port number of the WebSphere server. This should be the SOAP port for WebSphere 5.x.</p> <p><b>Default value:</b> 8880</p>



GUI Element	Description
<b>WEBSHERE_DIRECTORY</b>	<p>The path to the WebSphere directory that contains the /java and /lib subdirectories from the WebSphere Application Server.</p> <p>In WebSphere 6.x, this directory must also contain /profiles subdirectory. This subdirectory has all Key Store and Trust Store files needed for Global Security. The server profile in /profiles subdirectory must be called <b>default</b>. If the server profile has a different name, rename it to <b>default</b>.</p>
<b>WEBSHERE_PASSWORD</b>	<p>The password that SiteScope should use to login to WebSphere server.</p> <p>In WebSphere 6.x, Global Security is not supported in the solution template. This means that you can type in any text however, the text box cannot be left empty. If you need to work with Global Security, complete this template. Edit the WebSphere monitor and, in the Monitor Settings panel, update the Global Security boxes (<b>Trust store, Trust store password, Key store, Key store password</b>).</p>
<b>WEBSHERE_USER_NAME</b>	<p>The user name that SiteScope should use to login to WebSphere Application server.</p> <p>In WebSphere 6.x, Global Security is not supported in the solution template. This means that you can type in any text however, the text box cannot be left empty. If you need to work with Global Security, complete this template. Edit the WebSphere monitor and, in the Monitor Settings panel, update the Global Security boxes (<b>Trust store, Trust store password, Key store, Key store password</b>).</p>
<b>WEBSHERE_SERVER</b>	<p>The name of the server where the WebSphere Application is running. Do not type backslashes (\\) that indicate a UNC path as part of the name of the server.</p>
<b>Counters</b>	<p>The server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.</p>

GUI Element	Description
<b>Get Counters</b>	Click to open the Get Counters dialog box, and select the counters you want to monitor.
<b>Silent deployment</b>	<p>Select this option to submit the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to &lt;SiteScope root directory&gt;\logs\silent_deployment.log.</p> <p><b>Default value:</b> Not selected</p>
<b>Verify monitor properties with remote server</b>	<p>Select this option to verify the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed.</p> <p><b>Note:</b> When this option is selected, deployment time is slowed due to the remote connection.</p> <p><b>Default value:</b> Selected</p>

## Monitor Deployment Wizard

This chapter includes the main concepts, tasks and reference information for the Monitor Deployment Wizard.

---

**Note:** The Monitor Deployment Wizard is available only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center.

---

### **This chapter includes:**

#### **Concepts**

- ▶ Monitor Deployment Wizard Overview on page 1812
- ▶ Prerequisites for Running the Monitor Deployment Wizard on page 1814
- ▶ Monitor Deployment Wizard Templates and Variables on page 1816
- ▶ Full and Partial Monitor Coverage on page 1818
- ▶ Wizard Options on page 1819
- ▶ Monitor Deployment Wizard for Siebel on page 1820

#### **Tasks**

- ▶ Deploy Monitors Using the Monitor Deployment Wizard on page 1821

#### **Reference**

- ▶ Template Reference on page 1827
- ▶ Monitor Deployment Wizard User Interface on page 1835

## Monitor Deployment Wizard Overview

The Monitor Deployment Wizard provides a monitoring solution for existing Business Availability Center configuration item (CI) data using SiteScope templates. The wizard uses SiteScope templates to deploy monitors, groups, and remote servers with the existing and discovered CI data from the CMDB. For details on understanding CIs, see “Configuration Management Database (CMDB)” in *Model Management* in the HP Business Availability Center Documentation Library.

SiteScope templates enable you to deploy group and monitor configurations across multiple infrastructure elements with a minimal number of configuration steps. For details, see “SiteScope Templates” on page 1557.

The Monitor Deployment Wizard uses SiteScope’s template functionality to create a monitoring solution for the CIs in your CMDB. When you select CIs to monitor using the Monitor Deployment Wizard, the wizard automatically matches templates to the selected CIs based on the CI type selected. You can also select additional templates to apply to the selected CIs for your specific monitoring requirements. For details on which templates are deployed onto which CI types, see “Template Reference” on page 1827.

The CMDB may already include CI data that can be used for monitor deployment. These properties may have been entered while adding the CI to the IT Universe model or may have been discovered by the Discovery Manager. For details, see “Create CIs and Relationships in the CMDB” in *Model Management* in the HP Business Availability Center Documentation Library. The wizard is also able to retrieve the data from the CMDB for the selected CIs and use that data when deploying the SiteScope templates.

HP Business Availability Center enables you to use that data to create SiteScope monitors, groups, and remote servers for existing CIs in the CMDB.

The Monitor Deployment Wizard:

- ▶ enables you to select CIs onto which to deploy the SiteScope templates and recognizes which templates to deploy onto which CIs
- ▶ enables you to refine the selection of templates to deploy onto CIs

- checks the CI for existing monitors and measurements that match the monitoring solution to be deployed by the template and enables you to handle duplicate monitoring
- imports the configuration item's properties that have been defined in Universal CMDB Administration into the monitor's properties and creates remote servers on SiteScope
- uses template variables to enable you to enter data for monitor properties that are not imported from the configuration item's definition
- creates in the CMDB a **monitored by** relationship between the monitored CI and the created monitor

### Example of Monitor Deployment

For example, an Oracle database has been added as a CI to the IT Universe model in CMDB. You can use the Monitor Deployment Wizard to deploy the Oracle Database monitor onto the CI. The wizard imports the following properties that are defined for the server in the CMDB:

- database server IP address or server name
- database user name
- database password
- database port
- database SID

If a partial discovery was run during the Discovery and Dependency Mapping process, the wizard prompts you to enter values for some of the variables that are necessary for the deployment of the monitors.

## Prerequisites for Running the Monitor Deployment Wizard

Before running the Monitor Deployment Wizard, you must run the relevant discovery jobs to discover CIs and populate views. For details, refer to the *Discovery and Dependency Mapping Guide*.

After you have discovered the relevant CIs in your business environment, you can select one of the pre-defined views populated by the DDM jobs. Alternatively, you can create a view manually for the purpose of running the Monitor Deployment Wizard. We recommend creating a **Host Credentials** view which contains hosts with credentials. This can help to streamline the process of selecting the relevant hosts to be monitored in the Select CIs to Monitor step of the wizard.

---

**Note:** Do not create a view in which the same CI appears more than once. If you select a view in which the same CI appears more than once, the selection of the whole view in the wizard fails.

---

### To create a Host Credentials view:

- 1** Select **Admin > Universal CMDB > Modeling > View Manager**.
- 2** From the Views pane, right-click the Root folder in the tree.
- 3** Select **New** from the context menu. The Create New View dialog box opens.
- 4** Type **Host Credentials** in the View Name window.
- 5** From the CI Types pane, expand the System branch of the tree. Click and drag the Host CI type into the Editing pane.
- 6** From the CI Types pane, expand the Software Element branch of the tree. Click and drag the Shell CI type into the Editing pane.
- 7** Holding down the CTRL key, select both the Host and Shell nodes in the Editing pane. Right-click one of them and select **Add Relationship**. The Add Relationship dialog box opens.
- 8** In the Add Relationship dialog box, click **Advanced**. Select **Container Link** from the tree in the relationship window. Click **OK**.

- 9 Right-click the shell node in the Editing pane and select **Node Condition** from the context menu. The Node Condition dialog box opens.
- 10 In the Node Condition dialog box, clear the **Visible** check box and click **OK**.
- 11 Click the **Save** button from the toolbar to save the view.

For details on creating views, see “New View/View Properties/Save As View Wizard” in *Model Management* in the HP Business Availability Center Documentation Library.

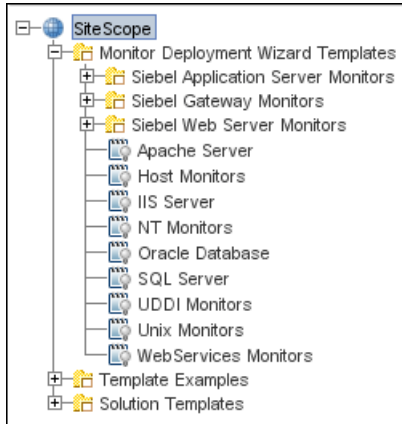
---

**Note:** In the Select CIs to Monitor step of the wizard, you can select CIs to monitor from many different views, but a specific CI may be selected only once, even if it appears in more than one view.

---

## Monitor Deployment Wizard Templates and Variables

The Monitor Deployment templates appear by default in the template tree in a container called **Monitor Deployment Wizard Templates**. This container and the templates and variables within it should not be edited or deleted.



Only advanced users with a thorough knowledge of working with templates should attempt to edit any of the variables or to add variables to the templates. For details, see “SiteScope Templates” on page 1557.

This section includes the following topics:

- ▶ “Monitor Template Variables” on page 1817
- ▶ “Selecting Templates” on page 1817
- ▶ “Manual Template Matches” on page 1817



## Monitor Template Variables

The templates associated with the selected CIs have variables which must be filled in before the wizard can deploy them. The system fills in most of the variables automatically by checking the CI information or the results of the Discovery and Dependency Mapping (DDM) process. Other variables are not filled in by the system because the data was missing from the CI information, the DDM process did not run completely, or because the data is dependent on the user. You must fill in the missing information for any selected monitor templates. You also have the option of not deploying the template by clearing the template selection if you do not know the variable values.

## Selecting Templates

Once a CI is selected, all the relevant templates are matched to the CI.

In the step for entering variable values, a check box appears next to each monitor template associated with that CI. By default, if there is any missing data for the variables in a template, that template is not selected for deployment. This enables the wizard to streamline the deployment process.

You can select or clear templates for deployment. If you select a template for deployment but fail to enter the missing data for its variables, an error message appears and the wizard cannot proceed until you enter the data. If you leave any templates unselected, a warning message appears to alert you that there are unselected templates but you can choose to proceed with the wizard anyway. This applies to all unselected templates, whether data was entered for them or not.

## Manual Template Matches

The wizard enables you to select other templates for deployment that were not automatically mapped by the wizard. For example, you may want to use an existing template that includes log file monitoring that is set to search for a specific string that would be relevant for host CIs in your environment. You can choose to deploy that template onto the host CIs you selected in the Select CIs to Monitor page.

You may also want to select a CI type that does not have a template associated with it and deploy an existing template onto that CI.

If you have matched additional monitor templates to be deployed onto CI types that are not in those predefined in the wizard, you can save these matches for future use when the same Business Availability Center user runs the wizard.

Also, if you removed templates that were matched by the wizard for specific CIs and chose to save matching, those templates are not matched to the selected CIs the next time the same Business Availability Center user runs the wizard.

For details, see “Save Matching” on page 1839.

## Full and Partial Monitor Coverage

For each selected CI, the Monitor Deployment Wizard checks whether the CI already has a monitored by relationship with any monitor CIs that are equivalent to the monitor instances that would result from the wizard deploying the templates mapped for that CI. It further checks the actual measurements within the monitor CIs and determines if the monitoring solution deployed by the wizard duplicates the monitors that exist for the selected CI.

If the CI onto which you want to deploy the monitoring solution already contains all of the same monitor and measurement instances, the CI is considered **fully covered**. If the CI has only part of the monitors and measurements already deployed, the CI is considered **partially covered**.

You can choose to clear fully or partially covered CIs and disable them for the deployment. Or, you have the option of continuing with the deployment and handling the duplicate monitors in the final step of the wizard. If, in the final step of the wizard, duplicate monitors on CIs were detected and the wizard successfully deployed templates onto these CIs, a **Handle Duplicates** button is displayed and enables you to delete these monitors, disable them or leave them in tact as duplicated monitors.

## Wizard Options

This section includes the following Monitor Deployment Wizard topics:

- “CI Group Hierarchy Option” on page 1819
- “SiteScope Remote Servers” on page 1819
- “Reporting” on page 1820

### CI Group Hierarchy Option

When you deploy templates using the Monitor Deployment Wizard, you can choose to create a CI group hierarchy which mirrors the CI hierarchy in the selected view in HP Business Availability Center. This means that SiteScope groups are created to correspond to the parent and grandparent CIs of the CI being monitored. These groups are arranged in a tree structure identical to the one that contains the actual CIs in the selected view in HP Business Availability Center.

### SiteScope Remote Servers

The SiteScope templates used in the Monitor Deployment Wizard are configured with template remotes which create remote server preferences in SiteScope for use by other SiteScope monitors. The remote servers created can be found in SiteScope under **Remote Servers > Microsoft Windows Remote Servers** (for Windows monitors) and **Remote Servers > UNIX Remote Servers** (for UNIX monitors). For details on remote servers, see “New/Edit Microsoft Windows Remote Server Dialog Box” on page 1291 and “New/Edit UNIX Remote Servers Dialog Box” on page 1299.

When the wizard deploys a template with remote server definitions for a physical monitor (for example, a CPU monitor), a remote preference is created with the name of the host (the host DNS name) plus the user name. When deploying a template with a remote server that already exists in SiteScope’s remote servers, SiteScope uses the existing remote and does not create another remote preference. For details on creating remote servers with templates, see “SiteScope Templates” on page 1557.

## Reporting

The final step of the Monitor Deployment Wizard consists of the Deployment Results page which displays information about the successful and unsuccessful monitor deployments. The report contains the names of the selected CIs and the monitors selected for deployment. The deployment status is indicated for each monitor.

The report can be exported to a PDF file. These reports include detailed information displaying all the created groups, monitors, and alerts, including the exact location where they can be found in SiteScope. These reports are useful for large deployments. For example, when hundreds of CIs are selected in the wizard, the resulting deployment can include thousands of new objects added to the SiteScope. For details, see “Deployment Results Page” on page 1842.

---

**Note:** After running the Monitor Deployment Wizard, the deployed monitors are not run immediately, but rather within the defined frequency scheduled for the monitor.

---

## Monitor Deployment Wizard for Siebel

You can use the Monitor Deployment Wizard to monitor your Siebel environment. The view to use for the wizard is the **Siebel Enterprise** view. The wizard can identify the Siebel configuration items in the CMDB and deploy a set of pre-configured monitors onto those items. The monitors include those that are specifically designed to monitor Siebel, as well as generic monitors that can monitor the performance of your Siebel network.

For details on the available templates used for the Siebel environment, see “Siebel Solution Templates” on page 1777.

For reference information on the Siebel monitor template and configuration items, see “Template Reference for Siebel” on page 1830.

## Deploy Monitors Using the Monitor Deployment Wizard

This task describes the steps involved in deploying monitors using the Monitor Deployment wizard.

This task includes the following steps:

- “Prerequisites” on page 1821
- “Run Discovery and Dependency Mapping” on page 1821
- “Run the Wizard” on page 1821
- “Enter Missing Data for Selected CIs” on page 1823
- “Check the Configuration Summary and Deploy Monitors” on page 1824
- “Review the Deployment Results and Export the Report” on page 1825

### 1 Prerequisites

To prevent configuration update conflicts, it is strongly recommended to disable the configuration files before running the Monitor Deployment Wizard. In the **Preferences** context, select **General Preferences** and make sure that the **Enable configuration files** check box is cleared (this the default setting).

### 2 Run Discovery and Dependency Mapping

Prior to deploying monitors with the Monitor Deployment Wizard, you must discover the CIs in your system and populate views.

We recommend that you create a Host Credentials view for the purpose of running the Monitor Deployment Wizard so that the necessary credentials exist to access the servers. For details on this topic, see “Prerequisites for Running the Monitor Deployment Wizard” on page 1814.

### 3 Run the Wizard

Begin running the wizard. For details on the user interface, see “Monitor Deployment Wizard” on page 1835. The first step is to select CIs to monitor using the View Explorer. For details on the user interface, see “Select CIs to Monitor Page” on page 1837.

After selecting CIs to monitor, you can select monitor templates to apply to them using the Templates Selection dialog box. For details on the user interface, see “Templates Selection Dialog Box” on page 1838.

### Example

#### Welcome

The Monitor Deployment Wizard deploys pre-configured templates onto the configuration items in your CMDB. The wizard:

- Enables you to deploy monitors onto selected CIs using pre-configured templates
- Imports the configuration item's properties from the CMDB into the monitor's properties
- Uses template variables to enable you to enter data for monitor properties

Getting Started:

- Select CIs from the views in your CMDB. Modify your selection to include only the CIs you want monitored.
- Enter the variable data required to deploy the templates. The wizard automatically imports the CI's properties from the CMDB and fills the template variables, it is required only to fill missing data.
- Review the configurations for all the monitors the wizard is creating for each CI in a selected view.

For more information, open the Help.

#### Select CIs to Monitor

Select a view and highlight a CI within the view. Click the right arrow to perform deployment on the highlighted CI. The tree on the right displays the selected CIs.

The screenshot shows the 'Select CIs to Monitor' dialog box. At the top, there is a 'View' dropdown menu currently set to 'NetworkTopology'. Below this, a tree view displays the contents of the selected view. The tree has a root node 'NetworkTopology' which is expanded to show three child nodes, each represented by a server icon and a text label: '16.44.49.0', '16.59.58.0', and '16.59.60.0'. The '16.44.49.0' node is highlighted with a blue selection bar. To the right of this tree is another tree view. Its root node is 'All', which is expanded to show a single child node '16.44.49.0'. Between the two tree views are three navigation arrows: a left-pointing arrow at the top, a right-pointing arrow in the middle, and a left-pointing arrow at the bottom. At the bottom of the dialog box, a small dialog box titled 'Templates Selection' is visible, partially overlapping the main interface.

## 4 Enter Missing Data for Selected CIs

On the third page of the wizard, select the monitor templates to deploy and enter any missing data for them. For details on the user interface, see “Enter Required Data for CIs Page” on page 1840.

### Example

#### Enter Required Data for Selected CIs

Enter the required data in the fields below to ensure the successful creation of all monitors. All fields must be filled.  
Only CIs that lack required data are expanded

CI	Variable	Value
IT Department		
<input checked="" type="checkbox"/> NT Monitors(37 pts)	host_dnsname	1.2.3.4
	host_username	user1
	host_password	*****
	nt_domain	domain1
16.59.57.155		
<input checked="" type="checkbox"/> Host Monitors(1 pts)	Host DNS Name	16.59.57.155
<input type="checkbox"/> NT Monitors(37 pts)	Host DNS Name	16.59.57.155
	host_username	
	host_password	
	nt_domain	

## 5 Check the Configuration Summary and Deploy Monitors

On the fourth page of the wizard, review the final configuration summary and select a SiteScope group on which to deploy the templates. Click **Finish** to complete the wizard and deploy the monitors. For details on the user interface, see “Final Configuration Summary Page” on page 1841.

### Example

#### Final Configuration Summary

In this page you can review the configuration before deployment.  
For each CI a list of templates is displayed together with a number of monitors and estimated license points per template.

Total number of license points available on SiteScope server is 9545 (required number of points is 29).

CI Name / Template Name	Monitors to be created	License Points
<input type="checkbox"/> app1 <ul style="list-style-type: none"> <li><input type="checkbox"/> lob1               <ul style="list-style-type: none"> <li><input type="checkbox"/> Host                   <ul style="list-style-type: none"> <li><input type="checkbox"/> Host Monitors</li> </ul> </li> </ul> </li> </ul>	1	1
<input type="checkbox"/> 16.59.61.0 <ul style="list-style-type: none"> <li><input type="checkbox"/> labm1amrnd06               <ul style="list-style-type: none"> <li><input type="checkbox"/> 16.59.61.134                   <ul style="list-style-type: none"> <li><input type="checkbox"/> NT Monitors</li> <li><input type="checkbox"/> Host Monitors</li> </ul> </li> </ul> </li> </ul>	1 1	27 1
<b>6 CIs with total of 3 templates</b>	<b>3</b>	<b>29</b>

Monitors will be deployed on the SiteScope Group:

SiteScope

Create CI group hierarchy (creates groups in SiteScope according to the CI hierarchy name under the selected deployment group)



## 6 Review the Deployment Results and Export the Report

On the last page of the wizard, review the results of the deployment and, if necessary, retry deploying those template that failed to deploy. In this page, you can also handle duplicate monitors that were deployed. Optionally, you can export the deployment results to a .pdf file. For details on the user interface, see “Deployment Results Page” on page 1842.

### Example

**Deployment Results**

**Summary of successful deployments:**  
 7 templates were deployed for 4 CIs  
 Total number of deployed monitors is: 7

CI Name	Object Name	Status
Siebel WSE	Siebel Web Server Extension	Failed to commit - uniqueness violation - the name 'Siebel Web Server Extension for labm1sbl03' exists in requested destination
	Siebel Web Server Extension for labm1sbl03	Unknown

Modify failed monitors properties and retry creation

Allows the user to disable or delete duplicate monitors

**Handle Duplicate Monitors**

Please select desired action for the duplicated monitors below.

CI Name / Monitor Name	Select Desired Action		
[-] ami-il.mercury.global - Fully monitored			
[-] Ping ami-il.mercury.global(Ping)	<input checked="" type="radio"/> Leave Intact	<input type="radio"/> Disable	<input type="radio"/> Delete
[-] Windows Resources on ami-il.mercury.global(Windows Resources)	<input type="radio"/> Leave Intact	<input checked="" type="radio"/> Disable	<input type="radio"/> Delete
[-] Windows Resources on ami-il.mercury.global(Windows Resources)	<input type="radio"/> Leave Intact	<input type="radio"/> Disable	<input checked="" type="radio"/> Delete
[-] Ping ami-il.mercury.global(Ping)	<input checked="" type="radio"/> Leave Intact	<input type="radio"/> Disable	<input type="radio"/> Delete
[-] crazy - Fully monitored			
[-] Windows Resources on crazy(Windows Resources)	<input type="radio"/> Leave Intact	<input checked="" type="radio"/> Disable	<input type="radio"/> Delete
[-] Ping crazy(Ping)	<input checked="" type="radio"/> Leave Intact	<input type="radio"/> Disable	<input type="radio"/> Delete
[-] Ping crazy(Ping)	<input type="radio"/> Leave Intact	<input checked="" type="radio"/> Disable	<input type="radio"/> Delete
[-] Windows Resources on crazy(Windows Resources)	<input type="radio"/> Leave Intact	<input type="radio"/> Disable	<input checked="" type="radio"/> Delete

## Template Reference

The Monitor Deployment Wizard is enabled by a series of templates preconfigured in the SiteScope monitor tree.

This section includes the following tables:

- “Template Reference Table” on page 1827
- “Template Reference for Siebel” on page 1830

### Template Reference Table

Following is a table listing all the configuration items onto which the Monitor Deployment Wizard can deploy templates. The table lists the templates and CI types, the monitors which are deployed, the monitor properties imported from the CMDB, and the variable definitions that are either imported from the CMDB or defined within the wizard.

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Apache server	Apache	Apache Server monitor	server name or IP address	application_IP
			application port (default value is 8080)	application_port
Host	Host	Ping monitor	dns name	host_dnsname
	Windows			
	UNIX			
	Network			
	Switch			
	Router			
	switch-router			

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Windows server	Windows	Microsoft Windows Resources monitor	dns name	host_dnsname
				host_password
				host_username
				nt_domain
UNIX	UNIX	CPU and Memory monitor, UNIX Remote server		connection_method
			dns name	host_dnsname
				host_os
				host_password
Microsoft IIS server	IIS	Microsoft IIS Server monitor	server name or IP address	application_IP
			host password	host_password
			user name	host_username
			NT domain	nt_domain
Microsoft SQL server	sqlserver	Microsoft SQL Server monitor	server name or IP address	application_IP
				nt_domain
				SqlServerHost Password
				SqlServerHost UserName

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Oracle database	Oracle	Oracle Database monitor	server name or IP address	application_IP
			application password (default value is manager)	application_password
			application user name (default value is system)	application_user name
			database port (default value is 1521)	database_dbport
			database SID	database_dbsid
UDDI	UDDI Registry	UDDI Server	data_name	data_name
			business_name	business_name
Web Services	Web Service	WSDL	method_name	method_name
				method_ns
			ParamUrl	ParamUrl
				port
			purl	purl
				service_name
			soap_action	soap_action
WsdUrl	WsdUrl			

## Template Reference for Siebel

Following are tables listing all the Siebel configuration items onto which the Monitor Deployment Wizard can deploy monitors. The Siebel templates are divided according to groups. The table lists the CI Templates and CI types, the monitors which are deployed, the monitor properties imported from the CMDB, and the variable definitions that are either imported from the CMDB or defined within the wizard.

### Siebel Application Server Monitor

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Application Server	Application Server	Siebel Application Server log	Server_Name	Server_Name
			Siebel_Root_Dir	Siebel_Root_Dir
			Siebel_Logical_Instance_Name	Siebel_Logical_Instance_Name
		Siebel Application Server	Application	Application
			Gateway	Gateway
			Enterprise	Enterprise
			Username	Username
			Server_Manager_Path	Server_Manager_Path
	PASSWORD	PASSWORD		
	Database	Siebel Enterprise Integration Manager process (growth rate)	Database_Connection_URL	Database_Connection_URL
			Database_Driver	Database_Driver
			Database_UserName	Database_UserName
			Database_Server_Name	Database_Server_Name
			PASSWORD	PASSWORD

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Application Server <i>cont'd</i>	Database <i>cont'd</i>	Siebel Transaction Logging process (is enabled)	Database_UserName	Database_UserName
			Database_Driver	Database_Driver
			Database_Connection_URL	Database_Connection_URL
			Database_Server_Name	Database_Server_Name
			Database_PASSWORD	Database_PASSWORD
		Siebel Transaction Router process (growth rate)	Database_UserName	Database_UserName
			Database_Driver	Database_Driver
			Database_Connection_URL	Database_Connection_URL
			Database_Server_Name	Database_Server_Name
			Database_PASSWORD	Database_PASSWORD
		Siebel Workflow Rules process (growth rate)	Database_UserName	Database_UserName
			Database_Driver	Database_Driver
			Database_Connection_URL	Database_Connection_URL
			Database_Server_Name	Database_Server_Name
			Database_PASSWORD	Database_PASSWORD

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Application Server Host	Host	Disk Space	Server_Name	Server_Name
		Ping	Server_Name	Server_Name
		Memory	Server_Name	Server_Name
		CPU	Server_Name	Server_Name
		Directory log	Server_Name	Server_Name
			Siebel_Root_Dir	Siebel_Root_Dir
		Service Siebel Server	Server_Name	Server_Name
			Enterprise	Enterprise
			Server_Logical_Instance_Name	Server_Logical_Instance_Name
		Directory	Server_Name	Server_Name
Siebel_Root_Dir	Siebel_Root_Dir			
Siebel Component	Siebel Component	Siebel Component log	alias	alias
			Server_Name	Server_Name
			Application	Application
			Siebel_Root_Dir	Siebel_Root_Dir
			Siebel_Logical_Instance_Name	Siebel_Logical_Instance_Name
		Siebel Component	alias	alias
			Username	Username
			Enterprise	Enterprise
			Application	Application
			Gateway	Gateway
			Server_Manager_Path	Server_Manager_Path
			Server_Logical_Instance_Name	Server_Logical_Instance_Name
			PASSWORD	PASSWORD
			Group_Name	Group_Name
			data_name	data_name



Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Component Group	Siebel Component Group	Siebel Component Group on	alias	alias
			Server_Logical_Instance_Name	Server_Logical_Instance_Name
			Enterprise	Enterprise
			Application	Application
			Gateway	Gateway
			data_name	data_name
			Server_Manager_Path	Server_Manager_Path
			Server_Name	Server_Name
PASSWORD	PASSWORD			

### Siebel Gateway Monitors

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Gateway Server Host	Host	CPU	Server_Name	Server_Name
		Directory	Server_Name	Server_Name
			Siebel_Root_Dir	Siebel_Root_Dir
		Disk Space	Server_Name	Server_Name
		Memory	Server_Name	Server_Name
		Ping	Server_Name	Server_Name
Service	Server_Name	Server_Name		

### Siebel Web Server Monitors

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Web Server Extension	Siebel Web Server Extension	Service	Server_Name	Server_Name
		Siebel Web Server	Server_Name	Server_Name
			Application	Application
			Username	Username
			PASSWORD	PASSWORD
		URL	Server_Name	Server_Name
			Application	Application
			Username	Username
			PASSWORD	PASSWORD
		Siebel Web Server Host	Host	CPU
Directory	host_dnsname			host_dnsname
	Siebel_Root_Dir			Siebel_Root_Dir
Disk Space	host_dnsname			host_dnsname
Memory	host_dnsname			host_dnsname
Ping	host_dnsname			host_dnsname
Service	host_dnsname			host_dnsname
Web Server	Web Server	Microsoft IIS Server	host_dnsname	host_dnsname
		Port 80	host_dnsname	host_dnsname

## Monitor Deployment Wizard User Interface

### This section includes:

- Monitor Deployment Wizard on page 1835

---

**Note:** The Monitor Deployment Wizard is available only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center.

---

## Monitor Deployment Wizard

<b>Description</b>	<p>Enables you to deploy SiteScope monitors using the configuration item data from the CMDB using pre-defined templates.</p> <p><b>To access:</b> Select <b>Admin &gt; System Availability Management</b>. Right-click the required SiteScope server or group and select <b>Monitor Deployment Wizard</b> or click the <b>Monitor Deployment Wizard</b> icon in the Summary page next to the required SiteScope server.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>➤ The wizard is accessible only if you have a running SiteScope hosted in System Availability Management Administration.</li> <li>➤ After running the Monitor Deployment Wizard, the deployed monitors do not begin to run immediately, but rather within the defined monitor running frequency time. You must give the system time to implement all the updates.</li> </ul>
<b>Included in Tasks</b>	<p>“Deploy Monitors Using the Monitor Deployment Wizard” on page 1821</p>

<b>Useful Links</b>	“Monitor Deployment Wizard” on page 1811
<b>Wizard Map</b>	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

 **Welcome Page**

<b>Description</b>	Describes the wizard.
<b>Important Information</b>	An error message appears when you attempt to proceed to the next page if: <ul style="list-style-type: none"> <li>▶ the SiteScope you selected is not available</li> <li>or</li> <li>▶ the CMDB is not available</li> </ul> For general information about the Monitor Deployment Wizard, see “Monitor Deployment Wizard” on page 1835.
<b>Useful Links</b>	“Work with the SiteScope Source Adapter – Workflow” in <i>Model Management</i> in the HP Business Availability Center Documentation Library.
<b>Wizard Map</b>	The Monitor Deployment Wizard contains: <b>Welcome Page</b> > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

 **Select CIs to Monitor Page**

<b>Description</b>	Enables you to select CIs onto which to deploy the SiteScope monitors.
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ If a CI appears under more than one view in the left pane, you cannot select it more than once in the selection that appears in the right pane, even if you attempt to select it from different views.</li> <li>▶ The wizard checks for full and partial monitor coverage of the selected CIs. You have the option of deploying the template onto these CIs and handling duplicate monitors.</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Monitor Deployment Wizard Templates and Variables” on page 1816</li> <li>▶ “Full and Partial Monitor Coverage” on page 1818</li> </ul>
<b>Wizard Map</b>	The Monitor Deployment Wizard contains: Welcome Page > <b>Select CIs to Monitor Page</b> > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):



GUI Element	Description
<View Explorer>	<p>The Select CIs to Monitor page uses the standard View Explorer functionality to select CIs in the left pane and move them to the right pane. For details, see “CI Selector User Interface” in <i>Model Management</i> in the HP Business Availability Center Documentation Library.</p> <p><b>Note:</b> The wizard cannot create monitors for the following CIs:</p> <ul style="list-style-type: none"> <li>▶ CIs that do not have a matching template for deploying a monitor type</li> <li>▶ CIs that are monitor CIs, generally those appearing in the monitor view</li> </ul> <p>If you selected any CIs of these types, a warning message appears when you attempt to proceed to the next step of the wizard.</p>

### **Templates Selection Dialog Box**

<b>Description</b>	<p>Enables you to apply templates to CI Types which were not automatically matched by the wizard.</p> <p><b>To access:</b> Click the <b>Templates Selection</b> button from the Select CI to Monitor step of the Monitor Deployment Wizard.</p>
<b>Important Information</b>	<p>The Monitor Deployment Wizard automatically matches templates to the CI Types of the selected CIs. You can add additional templates manually in this dialog box. The selected templates are added to all of the selected CI Types.</p>

<b>Useful Links</b>	“Monitor Deployment Wizard Templates and Variables” on page 1816
<b>Wizard Map</b>	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > ( <b>Templates Selection Dialog Box</b> ) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

<b>GUI Element</b>	<b>Description</b>
	Click to add the selected templates in the left pane to the CI selection in the right pane.
	Click to remove selected templates from the CI selection.
<Template list>	The left pane lists all the available templates in the wizard. The child objects are the monitors that are deployed by the template.
<CI Type Selection>	The right pane lists the CI Types of all the CIs selected in the Select CI to Monitor step of the Monitor Deployment Wizard. If the wizard was able to match templates to the selected CI Types, the CI Type is listed with the applicable template as a child object.
<b>Save Matching</b>	Select the check box to save your template selection as a preference. This includes those templates that are selected manual for CI types and those that are cleared from the automatic selection of the wizard. The manually adjusted templates selection is matched to the selected CIs automatically the next time the same Business Availability Center user runs the wizard.
<b>Restore Defaults</b>	Click to reset the list and remove all the added templates from the CI Types (those added automatically by the wizard remain).

 **Enter Required Data for CIs Page**

<b>Description</b>	Enables you to fine tune your template selection for specific CIs and fill in the missing information for those templates.
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ If data is missing for any selected templates, an error appears and you are unable to proceed to the next step.</li> <li>▶ If any templates are unselected, a warning appears before you proceed to the next step that informs you that there are unselected templates. This applies whether data is filled in for the unselected templates or not.</li> </ul>
<b>Wizard Map</b>	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > <b>Enter Required Data for CIs Page</b> > Final Configuration Summary Page > Deployment Results Page

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Expanded CI list>	The CIs that are missing required data are expanded. (If no CIs are missing data, this section does not appear.)
<Unexpanded CI list>	CIs that are not missing data are not expanded. You can optionally expand the CIs to modify the data. (If all CIs are missing data, this section does not appear.)
<b>CI column</b>	Each template for each CI is displayed separately with the relevant number of license points for that template. Select the check box for the CI and template combinations for which you want to deploy monitors.



GUI Element	Description
<b>Variable column</b>	The variables for templates with missing data are listed in the Variable column.
<b>Value column</b>	The missing data in the Value column for all the selected templates. You can tab between the fields and enter the required data in the available fields. You do not need to enter missing data for templates that are not selected.

### **Final Configuration Summary Page**

<b>Description</b>	Displays a list of the monitors about to be deployed and enables you to select the SiteScope group onto which they are deployed.
<b>Important Information</b>	Above the table, a note displays the total number of license points available on the SiteScope server (after the current action is complete). If the number of license points required for the current action exceeds your available points, a warning appears to tell you to remove some of the selected templates.
<b>Wizard Map</b>	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > <b>Final Configuration Summary Page</b> > Deployment Results Page

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element	Description
<b>CI Name/Template Name column</b>	Lists each selected CI with its templates.
<b>Monitors to be Created column</b>	Indicates the number of monitors being created for each template.
<b>License Points column</b>	Indicates the number of SiteScope license points required for each monitor.

GUI Element	Description
<b>SiteScope Group selection window</b>	<p>To select the SiteScope group under which the monitors are deployed, click <b>Browse</b> and select a group from the tree in the Choose Target SiteScope Group dialog box.</p> <p><b>Note:</b> If you attempt to deploy the same monitor on the same CI in the same group twice, the deployment fails with a unique name error. However, you may select a different group under which to deploy that monitor onto that CI.</p>
<b>Create CI group hierarchy</b>	<p>Select the check box to create a CI group hierarchy. This creates SiteScope groups under the target group with the identical hierarchy of the CIs. For details, see “CI Group Hierarchy Option” on page 1819.</p>

 **Deployment Results Page**

<b>Description</b>	Displays a summary of the successful and unsuccessful template deployments.
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The deployment of monitors occurs at the template level. This means that if the deployment fails for any of the template elements (monitor, group, remote, or alert), no other monitors in the template are deployed.</li> <li>▶ When you deploy a physical monitor (for example, a CPU monitor), a remote server with the same name is also created if such a remote server does not already exist under Remote Servers (Microsoft Windows or UNIX).</li> </ul>
<b>Wizard Map</b>	<p>The Monitor Deployment Wizard contains:</p> <p>Welcome Page &gt; Select CIs to Monitor Page &gt; (Templates Selection Dialog Box) &gt; Enter Required Data for CIs Page &gt; Final Configuration Summary Page &gt; <b>Deployment Results Page</b></p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Click to export the Monitor Deployment Wizard Summary page to a PDF. This report includes all created entities in SiteScope displaying the deployment directory and status. It also displays the status of duplicate monitors.</p>
<b>CI Name column</b>	Lists the names of the selected CIs.
<b>Object Name column</b>	Lists the monitors selected for deployment onto a given CI.
<b>Status column</b>	Indicates whether or not the deployment succeeded.
<b>Retry Failed Deployments</b>	<p>Click <b>Retry Failed Deployments</b> to re-attempt to deploy those monitors whose deployment failed by modifying the data entered in the Type Required Data for CIs page.</p> <p><b>Note:</b> This button appears only if there were failed deployments.</p>
<b>Handle Duplicate Monitors</b>	<p>If duplicate monitors were deployed, click <b>Handle Duplicate Monitors</b> to open the Handle Duplicate Monitors dialog box. For each duplicate monitor listed, you can select to leave it intact, disable it, or delete it. If all the monitors are to be handled in the same way, you can use the <b>Leave All Intact</b>, <b>Disable All</b> or <b>Delete All</b> buttons at the bottom of the page. For details on understanding duplicate monitors, see “Full and Partial Monitor Coverage” on page 1818.</p>



# Part VIII

---

## SiteScope Dashboard



---

## Working with SiteScope Dashboard

This chapter includes the main concepts, tasks, and reference information for SiteScope Dashboard.

### **This chapter includes:**

#### **Concepts**

- ▶ SiteScope Dashboard Overview on page 1848
- ▶ Dashboard Filter Overview on page 1849
- ▶ Acknowledging Monitor Status on page 1850
- ▶ Accessing SiteScope Tools on page 1851

#### **Tasks**

- ▶ Customize SiteScope Dashboard on page 1851
- ▶ Analyze Data in SiteScope Dashboard on page 1853

#### **Reference**

- ▶ SiteScope Dashboard User Interface on page 1856

## SiteScope Dashboard Overview

SiteScope monitoring provides a real-time picture of system availability and performance. You configure SiteScope monitors to collect metrics from a range of infrastructure components, including Web, application, database, and firewall servers. The status and metrics are then aggregated for presentation in SiteScope Dashboard.

Dashboard is linked to the SiteScope monitor tree hierarchy. The data displayed in Dashboard represents the selected context in the monitor tree. The highest level is the SiteScope node and any applicable monitor groups. The lowest-level element for display in a Dashboard view is an individual SiteScope monitor and its measurements.

Dashboard includes functions that you can use to customize the display of monitor information. This includes defining named filter settings to limit the display of data to those matching a defined criteria. You can also select various data display options.

Dashboard also includes hyperlinks and menus that you can use to navigate through the hierarchy of monitor elements, manually run a monitor, disable monitors, and access alert definitions.



## Dashboard Filter Overview

You can filter monitors or groups by the following criteria:

- ▶ monitor or group names containing a specific text string
- ▶ monitors or groups monitoring a specific host or server
- ▶ monitors or groups reporting an error
- ▶ measurement results containing a specific text string

Filters are applied primarily to monitors. The filter criteria are not applied to groups, alerts, or reports. You can use view settings to filter on other elements. For more information, see “Searching and Filtering SiteScope Objects Overview” on page 105.

Filters are applied to all Dashboard views. This means that some monitors may not be displayed depending on the filter criteria and the selected node. Generally, it is best to use filters together with the **Show All Descendent Monitors** view option. Filters remain active until you change or reset the filter criteria in the Dashboard Filter window.

Dashboard filters are separate from SiteScope tree filters. You can use either Dashboard filters or SiteScope tree filters to filter the display of nodes to specific monitor types. However, Dashboard filters are applied to the results of any currently selected tree filter setting. If a tree filter setting is active, this may prevent the Dashboard filter from finding monitors that match the filter criteria, even if such monitors do exist in the SiteScope environment.

You can save a filter setting by defining the filter settings and then saving the view as a Dashboard Favorite. For more information, see “Defining and Managing Filter Settings” on page 106.

For details on configuring a Dashboard filter, see “Dashboard Filter Dialog Box” on page 1871.

## Acknowledging Monitor Status

The acknowledgement function can be used to track resolution of problems that SiteScope detects in your system and network infrastructure. With this function, SiteScope keeps a record of when the problem was acknowledged, what actions have been taken, and by which user.

It also enables you to temporarily disable alerting on the monitors. This is useful to avoid redundant alerts while a problem is being actively addressed. You can also use the acknowledgement function as a simple trouble ticket system when more than one person uses SiteScope to manage system availability.

---

**Note:** The acknowledgement function is available only in Dashboard views. The acknowledgement icon is displayed only in Dashboard Detailed views.

---


You can add an acknowledgement to individual monitors or monitor groups. An acknowledgement added to a monitor applies only to that monitor. Any alert disable condition selected in the acknowledgement applies only to that monitor instance. Acknowledging a group applies the acknowledgement description and alert disable conditions to all monitors within the group. Acknowledgements applied to a group can be edited or deleted individually for monitors in the group.

Only one acknowledgement can be in force for a monitor or group at any given time. Acknowledgement comments and acknowledgement indicators continue to be displayed in the interface until they are deleted, even after any applicable alert disable schedule has expired.

Acknowledgement data and comments are written to a log file on the SiteScope machine. A new log entry is made each time you add, edit, or delete an acknowledgement. After a problem monitor or group is acknowledged, or the acknowledged status is cleared, you can view the history in the Acknowledge Log. The Acknowledge Log for an item can be viewed even if there is no acknowledgment currently in force.

For details on the Add Acknowledgment user interface, see “Add/Edit Acknowledge Dialog Box” on page 1867.

## Accessing SiteScope Tools

SiteScope contains a number of tools that can be used to test the monitoring environment. You can use these tools to query the systems you are monitoring and view detailed results of the action. This may include simply testing network connectivity or verifying login authentication for accessing an external database or service. You can run these tools directly from the Dashboard toolbar by clicking the **Tools**  button for the monitor (if diagnostic tools are available for the specific monitor).

For details on the different tools that are available, see “SiteScope Tools Overview” on page 193.

---

**Note:** SiteScope Tools option is available only for individual monitors.

---

## Customize SiteScope Dashboard

This task describes the steps involved in customizing the display and content of SiteScope Dashboard by setting the layout, configuring filters, and saving the view to favorites.

This task includes the following steps:

- “Set the Dashboard Layout” on page 1851
- “Select and Set a Dashboard Filter - Optional” on page 1852
- “Save View to Favorites” on page 1852

### **1 Set the Dashboard Layout**

Customize the display of group and monitor information using the settings on the Dashboard Settings dialog box.

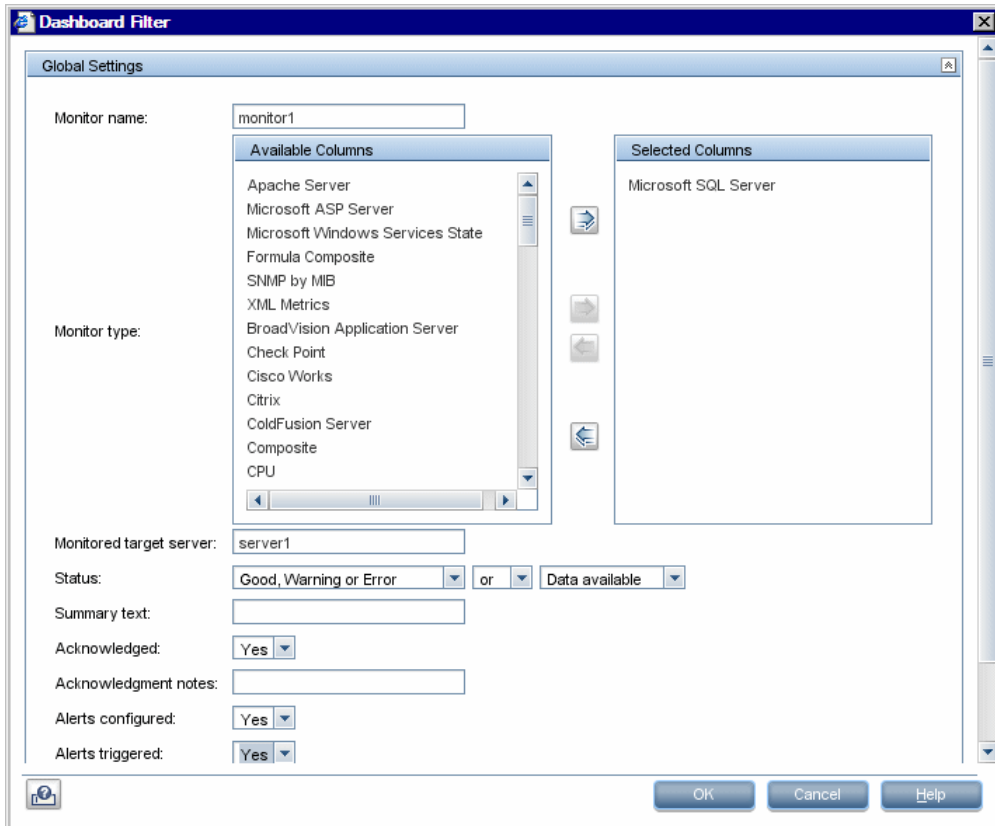
For details on the user interface, see “Dashboard Settings Dialog Box” on page 1875.

## 2 Select and Set a Dashboard Filter - Optional

Configure and set a Dashboard filter by selecting from the options available on the Dashboard Filter dialog box.

For details on the user interface, see “Dashboard Filter Dialog Box” on page 1871.

### Example



## 3 Save View to Favorites

After defining the Dashboard filter and layout settings, you can save them as a named favorite view in the Save to Favorites dialog box.

For details on the user interface, see “Save to Dashboard Favorites Dialog Box” on page 1869.

## Analyze Data in SiteScope Dashboard

This task describes the steps to follow to analyze data in SiteScope Dashboard.

This task includes the following steps:

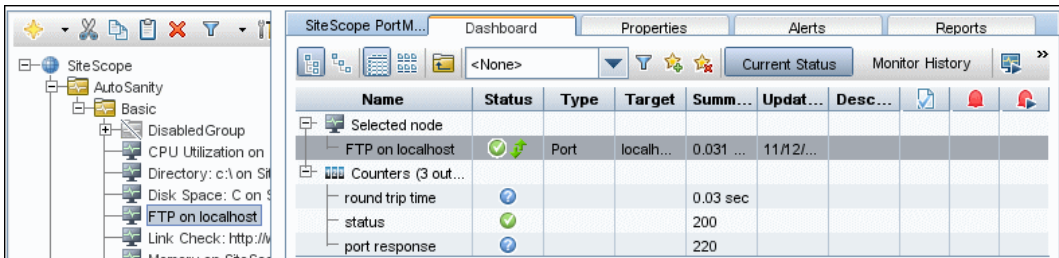
- “Drill Down to View Monitor and Measurement Status and Availability” on page 1853
- “View Configured and Triggered Alerts” on page 1854
- “Acknowledge Monitors” on page 1854
- “Monitor Your Microsoft Windows/UNIX Server’s Resources” on page 1855
- “View Monitor History” on page 1855





### 1 Drill Down to View Monitor and Measurement Status and Availability

When viewing SiteScope data in the Current Status view of Dashboard, you can drill down in the monitor tree to view monitor and measurement status and availability.


For details on navigating in the Dashboard, see “SiteScope Dashboard - Current Status View” on page 1857.

#### Example



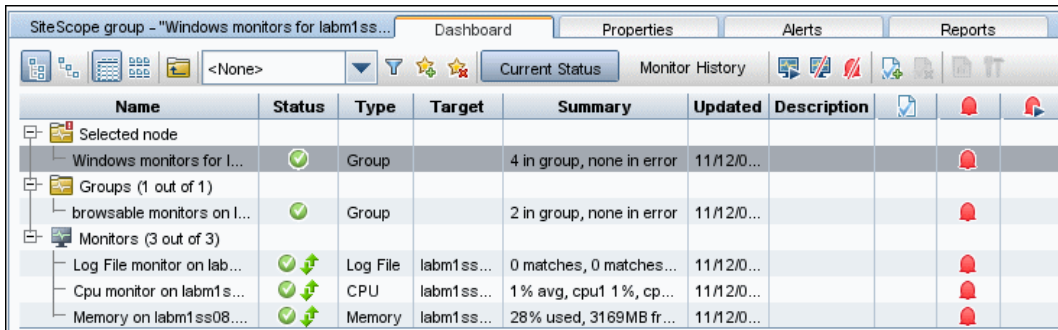
Name	Status	Type	Target	Summ...	Updat...	Desc...			
Selected node									
FTP on localhost		Port	localh...	0.031 ...	11/12/...				
Counters (3 out...)									
round trip time				0.03 sec					
status				200					
port response				220					

## 2 View Configured and Triggered Alerts

















You can view data about alerts in the configured alerts and triggered alerts columns. If alerts are configured for a monitor, you can double-click the **Configured Alert**  icon to see the list of configured alerts, and select an alert to view or edit the alert properties.

For details on the user interface, see “SiteScope Dashboard - Current Status View” on page 1857.


### Example



The screenshot shows the SiteScope Dashboard interface. The main table displays the following data:

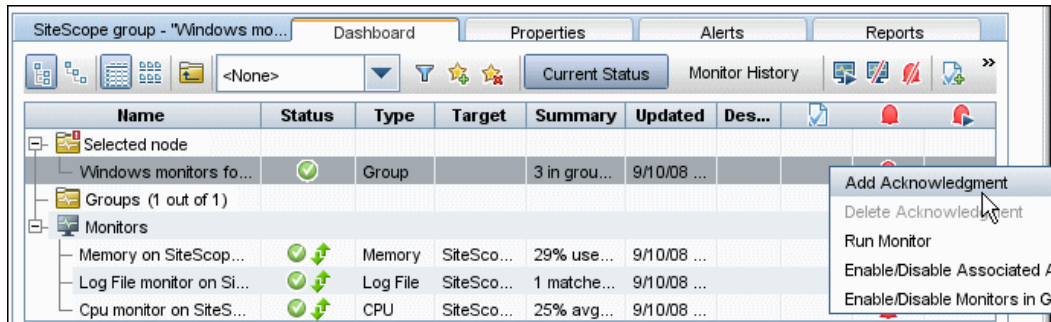
Name	Status	Type	Target	Summary	Updated	Description			
Selected node									
Windows monitors for labm1 ss...		Group		4 in group, none in error	11/12/0...				
Groups (1 out of 1)									
browsable monitors on labm1 ss...		Group		2 in group, none in error	11/12/0...				
Monitors (3 out of 3)									
Log File monitor on labm1 ss08...	 	Log File	labm1 ss...	0 matches, 0 matches...	11/12/0...				
Cpu monitor on labm1 ss08...	 	CPU	labm1 ss...	1% avg, cpu1 1%, cp...	11/12/0...				
Memory on labm1 ss08...	 	Memory	labm1 ss...	28% used, 3169MB fr...	11/12/0...				

## 3 Acknowledge Monitors

To acknowledge monitor status, click the **Add Acknowledgment**  icon or select **Add Acknowledgment** from the context menu, and enter the details in the Acknowledge dialog box.

For details on the user interface, see “Add/Edit Acknowledge Dialog Box” on page 1867.

### Example



## 4 Monitor Your Microsoft Windows/UNIX Server's Resources

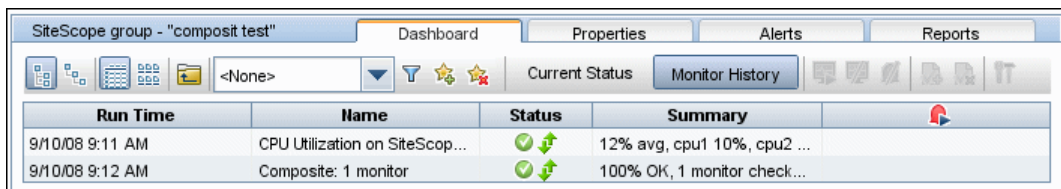
You can create a Microsoft Windows or UNIX Resources monitor to monitor your Windows or UNIX Server, and generating a Server-Centric report. For details on how to perform this task, see "Create a Server-Centric Report – Workflow" on page 1883.

## 5 View Monitor History

You enable and configure monitor history in the General Preferences. For details on the user interface, see "Dashboard Monitor History View Options" on page 1385.

To view monitor history, click the **Monitor History** button in SiteScope Dashboard. For details on the user interface, see "SiteScope Dashboard - Monitor History View" on page 1866.

### Example



## **SiteScope Dashboard User Interface**

**This section includes:**






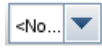
- ▶ SiteScope Dashboard - Current Status View on page 1857
- ▶ SiteScope Dashboard - Monitor History View on page 1866
- ▶ Add/Edit Acknowledge Dialog Box on page 1867
- ▶ Save to Dashboard Favorites Dialog Box on page 1869
- ▶ Delete Dashboard Favorites Dialog Box on page 1870
- ▶ Dashboard Filter Dialog Box on page 1871
- ▶ Dashboard Settings Dialog Box on page 1875
- ▶ Diagnostic Tools on page 1878
- ▶ Enable/Disable Monitor or Monitors in Group Dialog Box on page 1879




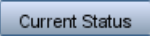
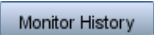









 **SiteScope Dashboard - Current Status View**




<b>Description</b>	<p>Displays current performance data for the infrastructure elements being monitored by SiteScope and provides access to functions you use to define filters.</p> <p>The Dashboard displays a table of groups and monitors for the element highlighted in the monitor tree or listed in the path. You can double-click each group or monitor node to navigate to child nodes and monitors.</p> <p>From the Dashboard, you can access the following SiteScope functions:</p> <ul style="list-style-type: none"> <li>▶ Server-Centric report</li> <li>▶ Preconfigured Quick Report</li> <li>▶ Acknowledge Monitor Status</li> <li>▶ Monitor Tools</li> <li>▶ SiteScope Health Status</li> <li>▶ Monitor History Information</li> <li>▶ Enable/Disable Monitors and Alerts</li> </ul> <p><b>To access:</b> Open the <b>Monitors</b> context. Select an object in the monitor tree, and click the <b>Dashboard</b> tab in the right pane.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ By default, the maximum number of objects that can be displayed in the Dashboard table for a selected element is 4000, and the maximum number of icons that can be displayed in Icon View is 700. You can modify these numbers by changing the values in the Dashboard Settings dialog box. However, we recommend that you use the default setting.</li> <li>▶ If the selected element has more lines than the maximum number that can be displayed in the Dashboard table, try creating a more restrictive tree filter or configure a Dashboard filter.</li> </ul>
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>▶ “Customize SiteScope Dashboard” on page 1851</li> <li>▶ “Analyze Data in SiteScope Dashboard” on page 1853</li> </ul>
<b>Useful Links</b>	<p>“SiteScope Dashboard Overview” on page 1848</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p><b>Show Child Groups and Monitors</b> displays only those elements that are direct children of the selected node. Subgroups and monitors are displayed in separate sections in the group and monitor status information area.</p>
	<p><b>Show All Descendent Monitors</b> displays all descendent monitors of the selected node. When the Icon view option is selected, only descendent monitor icons and names are displayed.</p>
	<p><b>Detailed View</b> displays groups and monitors in tabular list format with the element name, status, and other information arranged in individual table rows.</p>
	<p><b>Icon View</b> displays groups and monitors as an array of status icons with the name of the element below the icon.</p>
	<p>Click the <b>Up</b> button to go up one level in the monitor tree. This option is not available for SiteScope (the highest level in the tree).</p>
	<p>The Favorite box contains a drop-down list of the existing favorite views of Dashboard filter and layout settings. You can select the one you want to display in the Current Status or Monitor History view.</p> <p><b>Note:</b> The Favorites filter works on the monitor level which means that it does not filter groups. When working in the <b>Show Child Groups and Monitors</b> view, you can see groups that are not in a state that match the filter. To see only monitors in the filter, use the <b>Show All Descendent Monitors</b> view instead.</p> <p><b>Default value:</b> &lt;None&gt;</p>

GUI Element	Description
	<p>Click the <b>Manage Favorites</b> arrow, and select an option:</p> <ul style="list-style-type: none"> <li>▶ <b>Save to Favorites.</b> Opens the Save to Dashboard Favorites dialog box which enables you to save the current Dashboard filter and layout settings as a favorite view. For details on the user interface, see “Save to Dashboard Favorites Dialog Box” on page 1869.</li> <li>▶ <b>Delete Favorites.</b> Opens the Delete Dashboard Favorites dialog box which enables you to delete existing favorite views. For details on the user interface, see “Delete Dashboard Favorites Dialog Box” on page 1870.</li> </ul>
	<p>Click <b>Dashboard Filter</b> to open the Dashboard Filter dialog box. For details on the user interface, see “Dashboard Filter Dialog Box” on page 1871.</p>
	<p>Click <b>Dashboard Settings</b> to open the Dashboard Settings dialog box. For details on the user interface, see “Dashboard Settings Dialog Box” on page 1875.</p>
	<p>Displays a table of groups and monitors for the element highlighted in the monitor tree or listed in the path.</p>
	<p>Displays information about monitors, monitor groups, and alerts over the last 24 hours. This information is filtered by the number of hours, monitor status, and the number of data entries.</p> <p>For more information on viewing monitor history, see “SiteScope Dashboard - Monitor History View” on page 1866.</p>
	<p>Click <b>Run Monitors</b> to run the monitor or any monitors configured in the group. This opens an information window with the results.</p>



GUI Element	Description
	<p>Click <b>Enable/Disable Monitor</b> to open the Enable/Disable Monitor dialog box which enables you to enable or disable the monitor or all the monitors in the group, regardless of the setting in the monitor properties. If you select <b>Disable</b>, the monitors are disabled until you return to this dialog box and select <b>Enable</b>. For details on the Enable/Disable Monitor user interface, see “Enable/Disable Monitor or Monitors in Group Dialog Box” on page 1879.</p>
	<p>Click <b>Enable/Disable Associated Alerts</b> to open the Enable/Disable Associated Alerts dialog box which enables you to enable or disable all alerts associated with the monitor or all monitors in the group. For more details, see “Enable/Disable Associated Alerts” on page 374</p>
	<p>Click <b>Add Acknowledgment</b> to open the Add Acknowledge dialog box which enables you to add an acknowledgment to a monitor. For details on the Add Acknowledge user interface, see “Add/Edit Acknowledge Dialog Box” on page 1867.</p>
	<p>Click <b>Delete Acknowledgment</b> to delete the monitor’s acknowledgment.</p>
	<p>Click <b>Quick Report</b> to create a one-time SiteScope management report for the selected monitor. For more details on the report, see “Quick Report” on page 2076.</p>
	<p>Click <b>Tools</b> to open a diagnostic tool to test the selected monitoring environment. This button is available only for those monitor instances for which there is an appropriate diagnostic tool. For details on the SiteScope Tools, see “Diagnostic Tools” on page 1878.</p>








GUI Element	Description
	<p>The <b>Acknowledge</b> column indicates that a SiteScope user has acknowledged the current status of a monitor and may have temporarily disabled alert actions associated with that monitor. This icon is only displayed in Dashboard Detailed views. Moving the pointer over the icon displays the acknowledgment information as a tool tip. Double-click the icon to open the Edit Acknowledge dialog box. For details on this topic, see “Acknowledging Monitor Status” on page 1850. For details on the Add/Edit Acknowledge dialog box, see “Add/Edit Acknowledge Dialog Box” on page 1867.</p>
	<p>The <b>Configured Alerts</b> column indicates that one or more alerts are associated with the group or monitor. If you double-click the icon, a tooltip displays the configured alerts. Selecting an applicable alert definition name from the list opens the Edit Alert dialog box enabling you to view or edit the alert properties. For details on this topic, see “SiteScope Alerts” on page 1959.</p>
	<p>The <b>Triggered Alerts</b> column indicates that at least one alert has been triggered in the monitor. If no alert was triggered, the icon is not displayed. If a single alert was triggered, an icon representing the specific alert type is displayed. For a list of icons, see “Alert Actions” on page 2000.</p> <p>If multiple alerts were triggered, an icon representing multiple alerts is displayed. Clicking the alert icon displays alert details. The Triggered Alert column only appears for a table that contains monitors. For details on this topic, see “SiteScope Alerts” on page 1959.</p>
<p>&lt;Objects table&gt;</p>	<p>Lists the groups and monitors for the element highlighted in the monitor tree or listed in the path. You can double-click each group or monitor node to navigate to child nodes and monitors. Double-click a monitor to display the performance counters for that monitor.</p>

GUI Element	Description
<b>Name</b>	<p>A display name (alias) for the monitor instance or group. When a new group is created, you type its name. When a new monitor is created, you select its type from the list of available monitors. If you do not override this type in the <b>Name</b> box, the monitor is identified by the type of monitor. You can then optionally type an alias that helps you identify this monitor.</p>
<b>Status</b>	<p>A colored icon is displayed for each node in a Dashboard view, representing the operational status assigned to that component for its current performance level.</p> <p>A color-coded arrow is also displayed for each element in a Dashboard view, representing the data availability status of the monitor.</p> <p>You can point at the icons to display the monitor status and availability. For a description of the monitor status and availability icons, see “Status and Availability Levels” below.</p>
<b>Type</b>	<p>The type of monitor being displayed. You select the monitor type in the New Monitor page when you create the monitor instance.</p>
<b>Target</b>	<p>The <b>Target</b> column contains the name of the remote server containing the monitored object (if such a server exists). If, for example, the monitor type is CPU, then the target would be the name of the server on which the CPU being monitored is installed.</p> <p>The name displayed in the <b>Target</b> column can be either the system ID of the server or the user-assigned name (alias), depending on what was entered in the <b>Name</b> box when the server was added to the monitor tree.</p> <p>If the group contains a Microsoft Windows Resources monitor or UNIX Resources monitor, the server name in the Target column appears as a link. You can click the link to open the Server-Centric report for the server. For details on the user interface, see “Server-Centric Report” on page 1881.</p>

GUI Element	Description
<b>Summary</b>	<p>For monitors, the <b>Summary</b> column displays the most recent measurement results reported by the monitor. This may include more than one measurement, depending on the monitor type. For monitor groups, the summary displays the number of monitors within the group and the number of monitors, if any, that are reporting an error status.</p> <p>If a monitor has been disabled, it displays the disabled status (disabled manually or disabled until x time).</p>
<b>Updated</b>	<p>The date and time when the last event occurred in the group or monitor.</p>
<b>Description</b>	<p>The <b>Description</b> column can contain either text that describes the monitor or group or it can contain HTML that performs various actions when you click it.</p> <p>If this field contains text, you can double-click it to open a dialog box that displays the full description in HTML format.</p> <p>You can enter information in this column by selecting the monitor or group in the monitor tree and selecting the <b>Properties</b> tab. In the page that opens, expand <b>General Settings</b> and enter a description in the <b>Monitor/Group description</b> box.</p>

### Status and Availability Levels

Icon	Description
	<p><b>Good Status.</b> All performance measurements are within the Good threshold level.</p>
	<p><b>Warning Status.</b> At least one performance measurement is within the Warning range, but no measurements are within the Error or Poor range.</p>

Icon	Description
	<p><b>Error/Poor Status.</b> At least one performance measurement is within the Error or Poor range. This indicates either of the following:</p> <ul style="list-style-type: none"> <li>▶ The performance measurement has a value, but at poor quality level.</li> <li>▶ There is no measurement value due to some error.</li> </ul>
	<p><b>Status Not Defined (No Data).</b> There is no data for the group or monitor. This can be caused by any of the following reasons:</p> <ul style="list-style-type: none"> <li>▶ A new monitor has not yet run.</li> <li>▶ Monitor counters have not yet been collected.</li> <li>▶ The monitors on which the group or monitor depend are not reporting a Good condition.</li> </ul>
	<p><b>No Thresholds Breached Status.</b> No thresholds were defined for the monitor counter, so no status is assigned.</p>
	<p><b>Disabled Manually.</b> The group or monitor is currently disabled, and no data updates are being received.</p>
	<p><b>Data Collected Availability.</b> Indicates that SiteScope was able to connect to the remote system and perform the action defined by the respective monitor configuration. The resulting monitor status represents the results of the monitor action. If an error or warning is indicated, it represents an accurate measure of the target system's performance or the availability of the target resource.</p>
	<p><b>Availability Warning.</b> Indicates that SiteScope has detected a possible problem with the connectivity to the remote system.</p>
	<p><b>No Data Availability.</b> Indicates that SiteScope was not able to connect to the remote system. Any resulting error status for the respective monitor may be attributed to the failure to communicate with a remote server. It does not necessarily mean the target resource has failed.</p>



## Dashboard Context Menu


The following options are available by right-clicking in any column of a group object row:

GUI Element (A-Z)	Description
<b>Add Acknowledgment</b>	Opens the Acknowledge dialog box which enables you to add an acknowledgement to a monitor.
<b>Delete Acknowledgment</b>	Deletes the monitor's acknowledgement.
<b>Enable/Disable Associated Alerts</b>	Opens the Enable/Disable Alert Settings dialog box which enables you to enable or disable all the alerts for all monitors in the group. If you select <b>Disable</b> , the alerts are disabled until you return to this page and select <b>Enable</b> . For more details, see "Enable/Disable Associated Alerts" on page 374.
<b>Enable/Disable Monitor</b> <b>Enable/Disable Monitors in Group</b>	Opens the Enable/Disable Monitor Settings dialog box which enables you to enable or disable the monitor or all monitors in the group. If you select <b>Disable</b> , the monitors are disabled until you return to this page and select <b>Enable</b> . For details on the user interface, see "Enable/Disable Monitor or Monitors in Group Dialog Box" on page 1879.
<b>Quick Report</b>	Create a one-time SiteScope management report for the selected monitor over a given time period. For more details, see "Quick Report" on page 2076. <b>Note:</b> This menu item is displayed for monitors only.
<b>Run Monitor(s)</b>	Runs the selected monitor or all monitors in the selected group.
<b>Tools</b>	Opens a diagnostic tool that can help you troubleshoot monitor configuration problems. For details on the available tools, see "SiteScope Tools Overview" on page 193. <b>Note:</b> This menu item is displayed for monitors only, and is available only for specific monitors.

## SiteScope Dashboard - Monitor History View

<b>Description</b>	<p>Displays information about monitors, monitor groups, and alerts collected during the last 24 hours. This information is filtered by the number of hours, monitor status, and the number of data entries.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the Dashboard toolbar, click the <b>Monitor History</b> button.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ You enable this function in General Preferences.</li> <li>▶ You can determine exactly how much data you want saved for this function so that your database does not get overloaded.</li> <li>▶ By default, the maximum number of objects that can be displayed in the Monitor History table for a selected element is 4000, and the maximum number of icons that can be displayed in Icon View is 70. You can modify these numbers by changing the values in <b>Preferences &gt; Infrastructure Preferences &gt; Dashboard Settings</b>. However, we recommend that you use the default setting.</li> <li>▶ If the selected element has more lines than the maximum number that can be displayed in the Monitor History table, try creating a more restrictive tree filter or configure a Dashboard filter.</li> </ul>
<b>Included in Tasks</b>	“Customize SiteScope Dashboard” on page 1851
<b>Useful Links</b>	“Dashboard Monitor History View Options” on page 1385

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	The <b>Triggered Alert</b> icon appears next to any monitor that triggered an alert.
<b>Run Time</b>	The time the monitor ran.
<b>Name</b>	The name of the monitor.
<b>Status</b>	The monitor's status at runtime (Error, Warning, or Good). For details on the user interface, see "Status and Availability Levels" on page 1863.
<b>Summary</b>	The description of the monitor run.


## Add/Edit Acknowledge Dialog Box

<b>Description</b>	<p>Enables you to add or edit an acknowledgement for a monitor or monitor group.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the monitor view, right-click a monitor or group, and select:</p> <ul style="list-style-type: none"> <li>➤ <b>Add Acknowledgment</b> to add an acknowledgement to individual monitors or a monitor groups.</li> <li>➤ <b>Edit Acknowledgment</b> to edit an acknowledgment for a monitor or group that has been acknowledged.</li> </ul>
<b>Included in Tasks</b>	"Customize SiteScope Dashboard" on page 1851
<b>Useful Links</b>	"Acknowledging Monitor Status" on page 1850

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Acknowledge comment</b>	Enter an acknowledgement comment which is displayed as a tooltip associated with the acknowledgment icon in the Dashboard view and is recorded in the Acknowledge Log. You can update the comment as new information becomes available. The comment is displayed until the acknowledgment is deleted.
<b>Enable all associated alerts</b>	Enables all associated alerts (default setting).
<b>Disable all associated alerts for the next &lt;time period&gt;</b>	Disables alerting immediately and to continue suppressing alerting on the selected monitor or group for a duration that you specify.
<b>Disable all associated alerts on a one time schedule from &lt;timeA&gt; to &lt;timeB&gt;</b>	Disables alerting during a period of time that you specify. This can be useful if the system being monitored is expected to be unavailable during a certain period but you want to continue to run the monitor without triggering an alert.
<b>Disable description</b>	Enter an optional text description for alert icons associated with the monitors in the acknowledged context. The text description is added to the tool tip text that is displayed when the pointer is placed over any alert icon associated with the monitor in the Dashboard view. This text is displayed only while the alert disable option is in force. It is not written to the Acknowledge Log.
<b>View Acknowledge Log</b>	View all acknowledgment entries for the monitor or group from which you invoke the acknowledgment dialog box.


## Save to Dashboard Favorites Dialog Box

<b>Description</b>	<p>Enables you to define combinations of Dashboard filter and layout settings (which were selected using the Dashboard Filter dialog box and the Dashboard Settings dialog box) and save them as a named favorite view.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the Dashboard toolbar, click the arrow next to the <b>Manage Favorites</b>  button, and select <b>Save to Favorites</b>.</p>
<b>Important Information</b>	<p>Dashboard favorites are limited to settings that are applicable to Dashboard views. This means that Dashboard favorites do not save user-global view settings, or the context that was selected in the monitor tree when the favorite was saved.</p>
<b>Included in Tasks</b>	<p>“Customize SiteScope Dashboard” on page 1851</p>
<b>Useful Links</b>	<p>“SiteScope Dashboard Overview” on page 1848</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Name</b>	<p>Select an option for saving the current Dashboard filter and layout settings to favorites:</p> <ul style="list-style-type: none"> <li>▶ <b>Existing.</b> Enables you to replace one of the existing favorites with the current settings. Displays a list of the existing favorite views. By default, the list includes all the preconfigured favorites.</li> <li>▶ <b>New.</b> Enables you save the current settings to a new favorite view with the display name that you enter in the box.</li> </ul>


## Delete Dashboard Favorites Dialog Box

<b>Description</b>	Enables you to delete existing favorite views <b>To access:</b> Open the <b>Monitors</b> context. In the Dashboard toolbar, click the arrow next to the <b>Manage Favorites</b>  button, and select <b>Delete from Favorites</b> .
<b>Included in Tasks</b>	“Customize SiteScope Dashboard” on page 1851
<b>Useful Links</b>	“SiteScope Dashboard Overview” on page 1848

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Existing Favorites</b>	Select the view or views you want to delete from the list of current favorite views. By default, the list includes the following preconfigured favorites: <ul style="list-style-type: none"> <li>➤ All Objects</li> <li>➤ Disabled</li> <li>➤ Errors Only</li> <li>➤ Errors and Warnings</li> <li>➤ Good</li> <li>➤ Good and Warnings</li> <li>➤ No Data</li> <li>➤ Warnings Only</li> </ul>

## Dashboard Filter Dialog Box

<b>Description</b>	Enables you to configure a Dashboard filter by entering match criteria and selecting from the menu options. <b>To access:</b> Open the <b>Monitors</b> context. In the Dashboard toolbar, click the <b>Dashboard Filter</b>  button.
<b>Important Information</b>	Any combination of filter options can be included in a single filter. For example, the filter definition can filter on a combination of <b>Monitor type</b> , <b>Monitored target</b> , and <b>Status</b> .
<b>Included in Tasks</b>	“Customize SiteScope Dashboard” on page 1851
<b>Useful Links</b>	“Dashboard Filter Overview” on page 1849

### Global Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Monitor name</b>	Enter a text string or regular expression that matches the name of one of more monitors. When you apply this filter to the Dashboard view, only the monitors that match the <b>Monitor name</b> criterion are displayed.
<b>Monitor type</b>	Use this list to create a filter to display only selected monitor types.
<b>Monitored target server</b>	Enter the server name to filter monitors based on a particular host or server being monitored.

GUI Element	Description
<b>Status</b>	<p>Use this option to filter monitors by reported status. The status filter criterion can be defined in terms of monitor category status.</p> <p>The following status options are available:</p> <ul style="list-style-type: none"> <li>➤ <b>Any Status.</b> Show all monitors with any status. This is the default option. This can be used in combination with the <b>Data Available</b> option to filter out monitors that are in error due to connectivity or availability factors.</li> <li>➤ <b>Disabled.</b> Show only monitors reported as disabled.</li> <li>➤ <b>Error.</b> Show only monitors reporting an error status.</li> <li>➤ <b>Good.</b> Show only monitors reporting a good or OK status.</li> <li>➤ <b>Good, Warning, or Error.</b> Show all monitors except those reported as disabled.</li> <li>➤ <b>Warning.</b> Show only monitors reporting a warning status.</li> <li>➤ <b>Warning or Error.</b> Show only monitors reporting a warning or error status.</li> <li>➤ <b>Warning or Good.</b> Show only monitors reporting a warning or good status.</li> </ul> <p><b>Example:</b> Create a filter that displays only those monitors reporting a warning or error.</p>



GUI Element	Description
<b>Status (with Availability)</b>	<p>Use this option to create a compound filter by combining the monitor status category with the data availability status.</p> <p>The following data availability status options are available:</p> <ul style="list-style-type: none"> <li>▶ <b>Data Available.</b> Show monitors for which data is available, meaning the monitor was able to retrieve measurements from the target system.</li> <li>▶ <b>Data Unavailable.</b> Show monitors for which data is not available, meaning SiteScope was not able to retrieve measurements from the target system.</li> </ul> <p><b>Example:</b> Create a filter that displays only those monitors reporting <b>Error</b> and <b>Data Available</b>. This means that the filter shows monitors that indicate an error status for which the monitor was able to receive data from the monitored system as opposed to monitors that are reporting an error because the monitor was not able to communicate with the monitored system (that is, <b>Data Unavailable</b>).</p>
<b>Summary text</b>	<p>Use this option to filter monitors based on text included in their summary string. You can type a literal text string or a regular expression to match a text pattern.</p> <p>For details about regular expressions see “Using Regular Expressions” on page 261.</p>
<b>Acknowledged</b>	<p>Use this option to filter monitors based on their Operator Acknowledgment status. To filter on monitors that have been acknowledged, select <b>Yes</b> from the drop-down menu. To filter on unacknowledged monitors, select <b>No</b> from the drop-down menu.</p>
<b>Acknowledgment notes</b>	<p>Use this option to filter monitors based on text that may appear in their Operator Acknowledgment notes. You can type a literal text string or a regular expression to match a text pattern.</p> <p>For details about regular expressions see “Using Regular Expressions” on page 261.</p>


GUI Element	Description
<b>Alerts configured</b>	Use this option to filter monitors based on whether alerts have been configured on them. To filter on monitors that have one or more alerts configured on them, select <b>Yes</b> from the drop-down menu. To filter on monitors that do not have configured alerts, select <b>No</b> from the drop-down menu.
<b>Alerts triggered</b>	Use this option to filter monitors based on whether they have triggered an alert event. To filter on monitors that have generated one or more alerts, select <b>Yes</b> from the drop-down menu. To filter on monitors that have not generated alerts, select <b>No</b> from the drop-down menu.

## Monitor History Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Display time period</b>	Select the time frame for past events. <b>Default value:</b> Past 1 hour
<b>Monitor run status</b>	Select the required event status, relational operator, and data availability. <b>Default value:</b> Any

## Dashboard Settings Dialog Box

<b>Description</b>	<p>You use the Dashboard Settings dialog box to customize the display of group and monitor data in the Dashboard views. This allows you to enable or suppress the display of monitor measurement details, alert information, and acknowledgement functions.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the Dashboard toolbar, click the <b>Dashboard Settings</b>  button.</p>
<b>Important Information</b>	<p>Layout options apply only to the Detailed view. They are ignored when using the Icon view.</p>
<b>Included in Tasks</b>	<p>“Customize SiteScope Dashboard” on page 1851</p>
<b>Useful Links</b>	<p>“Dashboard Filter Overview” on page 1849</p>

## Dashboard Table Layout

The following elements are included (unlabeled GUI elements are shown in angle brackets>):


GUI Element	Description
<b>Lock columns</b>	<p>Select to lock the order of the table's columns. Clear the setting to change the table column order by dragging the column header to the right or the left.</p> <p><b>Default value:</b> Not selected</p>
<b>Table Columns</b>	<p>You use the Table Columns list to select optional columns to be displayed in the detailed tables. Your selections are applied to all applicable group and monitor elements.</p> <p>The columns available for display are:</p> <ul style="list-style-type: none"> <li>➤ Type</li> <li>➤ Summary</li> <li>➤ Alerts Triggered</li> <li>➤ Alerts Configured</li> <li>➤ Description</li> <li>➤ Status</li> <li>➤ Target</li> <li>➤ Ack(nowledged)</li> <li>➤ Updated</li> <li>➤ Name</li> </ul> <p><b>Default value:</b> All the properties are selected</p> <p>For details on the columns, see “SiteScope Dashboard - Current Status View” on page 1857</p>

## Dashboard Properties


The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Show monitor availability</b>	Select to show monitor availability icons in the Dashboard that indicate whether SiteScope was able to connect to a remote system or if a remote system was unavailable due to a connection problem. <b>Default value:</b> Not selected.
<b>Maximum dashboard objects</b>	The maximum number of objects that can be displayed in the Dashboard table for a selected element. <b>Default value:</b> 4000 <b>Note:</b> If the selected element has more objects than the maximum number that can be displayed, you should try to create a more restrictive tree filter or configure a Dashboard filter instead of increasing this setting.
<b>Maximum dashboard icons</b>	The maximum number of icons that can be displayed in the Dashboard's Icon View. <b>Default value:</b> 700 <b>Maximum recommended value:</b> 1500 <b>Note:</b> If the selected element has more icons than the maximum number that can be displayed, you should try to create a more restrictive tree filter or configure a Dashboard filter instead of increasing this setting.
<b>Dashboard refresh rate (in seconds)</b>	The amount of time, in seconds, to wait between refreshing the Dashboard. <b>Default value:</b> 60 seconds <b>Minimum value:</b> 30 seconds

## Diagnostic Tools

<b>Description</b>	<p>The diagnostic tools view represents the utilities that are useful to test the monitoring environment. Use these tools to make a variety of requests and queries of systems you are monitoring and to view detailed results of the action.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the Dashboard, select a monitor instance for which a diagnostic tool is available, and click the <b>Tools</b>  button.</p>
<b>Important Information</b>	<p>You can see the list of diagnostic tools that are available in SiteScope by clicking the <b>Tools</b> button in the left pane.</p>
<b>Useful Links</b>	<p>“SiteScope Tools Overview” on page 193</p>

## Enable/Disable Monitor or Monitors in Group Dialog Box

<b>Description</b>	<p>Enables you to select an option for enabling or disabling the monitor or all the monitors in the group, regardless of the individual monitor setting in the monitor properties tab. If you select <b>Disable monitor/monitors in group</b>, the monitors are disabled until you return to this dialog box and select <b>Enable monitor/monitors in group</b>.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the Dashboard, select a monitor or group, and click the <b>Enable/Disable Monitor</b>  button.</p>
<b>Important Information</b>	<p>If you disable a monitor or group using the <b>Disable monitor/monitors in group</b> option, the Dashboard shows disabled manually as the status in the <b>Summary</b> column for the affected objects. You must enable any object with a disabled manually status before you can set objects to be disabled for a specific period of time. This is also true at the group level. For example, if monitors in a group are disabled for a time period and monitors in a subgroup of that group have the disabled manually status, the subgroup monitors remain disabled even after the disable time period has lapsed for the parent group.</p>
<b>Useful Links</b>	<p>“Enable/Disable Monitor” on page 373</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Enable monitor/monitors in group</b>	<p>If the monitor/monitors in the group have previously been disabled in the monitor properties, select to enable the monitor/monitors in the group.</p> <p><b>Default value:</b> Selected</p>
<b>Enable temporarily disabled monitor only/monitors in group</b>	<p>If the monitor/monitors in the group have previously been disabled temporarily in the monitor properties, select to enable the monitor/monitors in the group.</p>

GUI Element	Description
<b>Disable monitor/monitors in group</b>	When a monitor/monitors in the group have been disabled, SiteScope continues to schedule the monitor/monitors in the group to run based on the <b>Frequency</b> setting for the monitor but the monitor action is not run. SiteScope records a monitor data log entry for the monitor/monitors in the group when it was scheduled to be run but reports the monitor status as disabled in the place of measurement data.
<b>Disable monitor/monitors in group for the next &lt;time period&gt;/Disable</b>	Enter a time period that the monitor/monitors in the group should remain disabled. Select <b>Seconds</b> , <b>Minutes</b> , <b>Hours</b> , or <b>Days</b> to define the disable time period as applicable.
<b>Disable monitor/monitors in group on a one time schedule from &lt;time&gt; to &lt;time&gt;</b>	Use this option to temporarily disable the monitor/monitors in the group for a time period in the future. The time period can span more than one day. Enter or select the start time and end time for the disable period using the format: hh:mm:ss mm/dd/yyyy.
<b>Disable description</b>	Enter optional descriptive text. This description appears as part of the monitor status in the monitor group display. The disable status text also includes a string indicating which disable option is in force for the monitor, for example Disabled manually indicates that the monitor was disabled using the <b>Disable monitor</b> option.



# 153

---

## Server-Centric Report

This chapter includes the main concepts, tasks, and reference information for the Server-Centric report.

### **This chapter includes:**

#### Concepts

- ▶ Generating a Server-Centric Report on page 1881

#### Tasks

- ▶ Create a Server-Centric Report – Workflow on page 1883
- ▶ Create a Server-Centric Report – Scenario on page 1885

#### Reference

- ▶ Server-Centric Report Measurements on page 1889
- ▶ Server-Centric Report on page 1890

### **Generating a Server-Centric Report**

For Microsoft Windows and UNIX Resources monitors you can create a Server-Centric report which displays data from three different metrics about the server being monitored. We recommend that you use Solution Templates when creating the Microsoft Windows or UNIX Resources monitor. For details on the Solution Templates, see:

- ▶ “AIX Host Solution Templates” on page 1679
- ▶ “Linux Host Solution Templates” on page 1719

- “Solaris Host Solution Templates” on page 1789
- “Microsoft Windows Host Solution Template” on page 1747

You can define the monitor manually by selecting **Enable Server-Centric report** in the required monitor settings page, as described in “Microsoft Windows Resources Monitor Settings” on page 720 and “UNIX Resources Monitor Settings” on page 937. When defining the monitor manually, you must select the required metrics for the monitors, according to the table in “Server-Centric Report Measurements” on page 1889.

The report displays the following metrics on the same graph:

- **CPU Utilization.** For UNIX Resource Monitors, this metric is calculated as an average of three counters: system processing utilization, user processing utilization, and input/output processing utilization. For Microsoft Windows Resources Monitors, the metric is calculated as processing capacity used out of total processing capacity.
- **Memory Utilization.** Calculated as memory used out of total available memory.
- **Network Utilization.** Calculated by system-specific counters. Calculating network utilization is supported only for Windows servers.

Each metric is displayed by a separate line of a unique color on the graph. The report enables you to easily make a visible correlation between the different metrics.

The report includes tables listing the top five processes by CPU utilization and memory consumption. You can navigate the graph and change the time of the data displayed in the tables. This enables you to focus in on a problematic period in the graph to locate the processes running at that time. For details on the Server-Centric report interface, see “Server-Centric Report” on page 1890.

The report also includes the Annotation Tool that enables you to annotate a snapshot of the report you are viewing, to highlight important areas. You can save, print, or email an annotation report. For details on the user interface, see “Annotation Tool” on page 2085.

For details on how to generate a Server-Centric report, see “Create a Server-Centric Report – Workflow” on page 1883.

## **Create a Server-Centric Report – Workflow**

This task describes the steps involved in creating a monitor to monitor your Windows and UNIX server, and generating a Server-Centric report.

For a scenario of this task, see “Create a Server-Centric Report – Scenario” on page 1885.

This task includes the following steps:

- “Create a Microsoft Windows or UNIX Resources Monitor” on page 1883
- “Generate the Server-Centric Report” on page 1884
- “Analyze Data in the Report” on page 1884

### **1 Create a Microsoft Windows or UNIX Resources Monitor**

To monitor your Microsoft Windows or UNIX server, you must create a Microsoft Windows or UNIX Resources monitor. You can create the monitor manually or by using solution templates. We recommend that you create a monitor using solution templates, as they contain all the required measurement counters.

For details on the Solution Templates, see:

- “Microsoft Windows Host Solution Template” on page 1747
- “AIX Host Solution Templates” on page 1679
- “Linux Host Solution Templates” on page 1719
- “Solaris Host Solution Templates” on page 1789

For details on creating a Microsoft Windows Resources or UNIX Resources monitor manually, see:

- “Microsoft Windows Resources Monitor Settings” on page 720.
- “UNIX Resources Monitor Settings” on page 937.

Make sure to select **Enable Server-Centric Report** and select the required measurements. For details on the measurements, see “Server-Centric Report Measurements” on page 1889.

## 2 Generate the Server-Centric Report

To monitor your server, navigate to Dashboard, display the data for the applicable Microsoft Windows or UNIX Resources monitor, and click the server name in the **Target** column in the row that corresponds to your resources monitor. The Server-Centric report opens.

## 3 Analyze Data in the Report

The report enables you to view three different metrics of your server in the same graph – CPU utilization, memory utilization, and network utilization. It also lists the top five processes by CPU utilization and memory consumption. You can drill down to specific times by clicking a data point on the graph.

For details on the Server-Centric report user interface, see “Server-Centric Report” on page 1890.

## Create a Server-Centric Report – Scenario

This scenario describes how to create a Server-Centric report.

For a task of this scenario, see “Create a Server-Centric Report – Workflow” on page 1883.

This task includes the following steps:

- ▶ “Configuring a Remote Server” on page 1885
- ▶ “Deploying a Microsoft Windows Host Solution Template” on page 1886
- ▶ “Creating a Server-Centric Report” on page 1887

### 1 Configuring a Remote Server

David Foster, a SiteScope user at NewSoft Company, wants to create a report that provides data on CPU utilization, memory utilization, and network utilization for a monitored server, Apollo.

Before he creates the report, David configures SiteScope to monitor the remote Windows server, Apollo, and configures the server in Microsoft Windows Remote Servers.

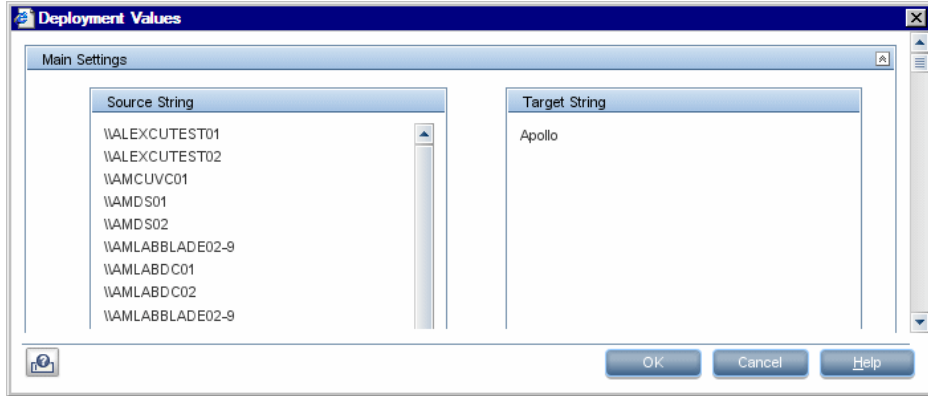


The screenshot shows the 'Main Settings' dialog box with the following configuration:

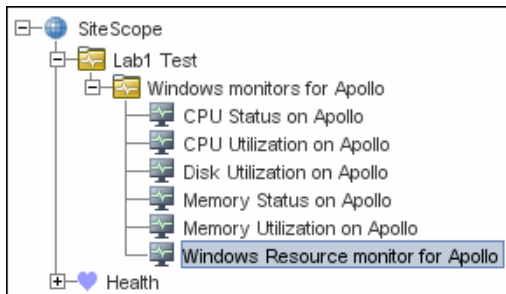
- Server:** \* \Apollo
- Credentials:**
  - Use user name and password
    - User name: administrator
    - Password: \*\*\*\*\*
  - Select predefined credentials
    - Credential profile: [dropdown]
    - Add Credentials button
- Trace
- Method:** \* NetBIOS [dropdown]
- Remote server encoding:** Cp1252 (windows-1252) [dropdown]

## 2 Deploying a Microsoft Windows Host Solution Template

After enabling SiteScope to monitor data on Apollo, David deploys the Microsoft Windows Host solution template into the selected group container, and selects Apollo as the server to monitor. David uses the solution templates when creating the Microsoft Windows Resource monitor, because the required monitors and metrics for generating a Server-Centric report are already configured.



After David deploys the solution template, SiteScope creates a group named Windows monitors for Apollo that contains the Microsoft Windows Resources monitor.

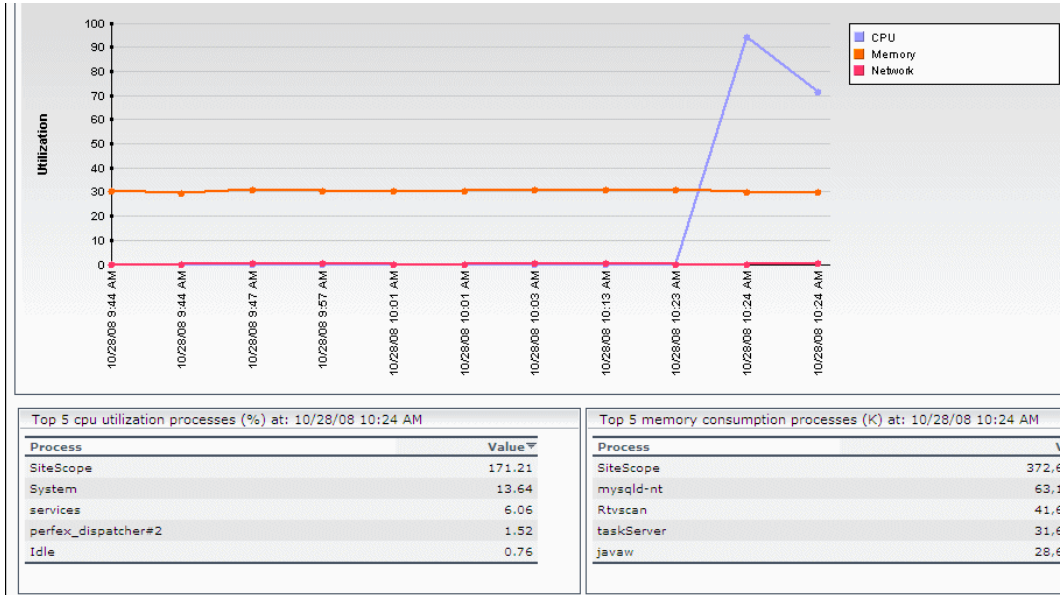


### 3 Creating a Server-Centric Report

David generates the Server-Centric report for Apollo from the Current Status view of Dashboard.

Name	Status	Type	Target	Summary	Updated
Selected node					
Windows monitors for Apollo	✓	Group		6 in gro...	10/28/0...
Groups (1 out of 1)					
Monitors					
Memory Status on Apollo	✓ ↑	Memory	Apollo	24% us...	10/28/0...
Memory Utilization on Apollo	✓ ↑	Microsoft Windows Resources	Apollo	Memory...	10/28/0...
CPU Utilization on Apollo	✓ ↑	Microsoft Windows Resources	Apollo	Proces...	10/28/0...
CPU Status on Apollo	✓ ↑	CPU	Apollo	0% avg...	10/28/0...
Windows Resource monitor...	✓ ↑	Microsoft Windows Resources	<a href="#">Apollo</a>	Memory...	10/28/0...
Disk Utilization on Apollo	✓ ↑	Microsoft Windows Resources	Apollo	Logical...	10/28/0...

The Server-Centric report opens, displaying the CPU Utilization, Memory Utilization, and Network Utilization metrics on the same graph. David can use this data to view the top processes by CPU utilization and memory consumption during different times, and focus in on problematic periods to locate the processes running at that time.





## Server-Centric Report Measurements

The following table displays the counters which must be selected when defining the monitor for the Server-Centric report manually:

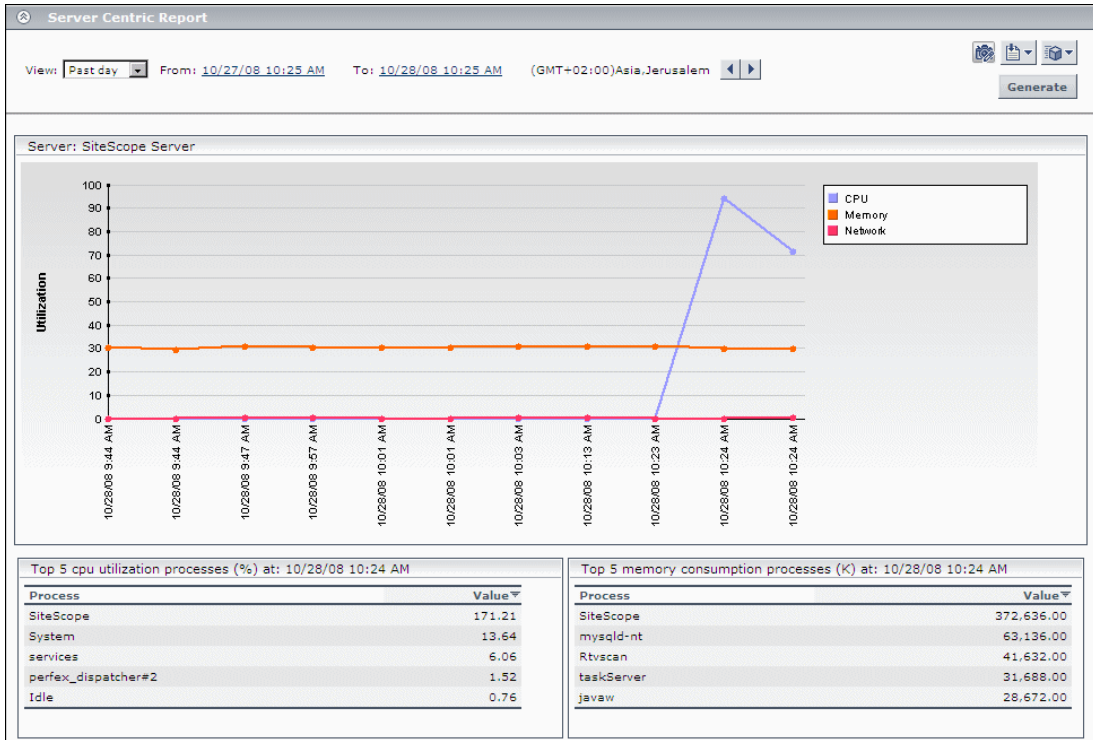
OS Type	Server-Centric Mandatory Counters
Counters for Microsoft Windows Resource Monitor	Memory\% Committed Bytes In Use
	Processor\_Total\% Processor Time
Counters for UNIX Resource Monitor on Solaris Platform	CPU utilization\%sys
	CPU utilization\%usr
	CPU utilization\%wio
	Memory\swap_avail
	Memory\swap_resv
Counters for UNIX Resource Monitor on AIX Platform	Processor\Total\%sys
	Processor\Total\%usr
	Processor\Total\%wio
Counters for UNIX Resource Monitor on Linux Platform	Memory\MemFree
	Memory\MemTotal
	Processor\Total\System
	Processor\Total\User
	Processor\Total\User low

For details on selecting counters for monitor definition, see:

- “Microsoft Windows Resources Monitor Settings” on page 720 (for Microsoft Windows Resources monitor counters).
- “UNIX Resources Monitor Settings” on page 937 (for Solaris, AIX, and Linux platforms).

## Server-Centric Report






The following is an example of the Server-Centric report.



<b>Description</b>	<p>A graphical report showing the metrics CPU utilization, memory utilization, and network utilization for a selected server.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. Click the server name link in the <b>Target</b> column of SiteScope Dashboard for a Microsoft Windows Resources or UNIX Resources monitor.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ This report is available only on those servers being monitored by a dedicated Microsoft Windows Resources monitor or UNIX Resources monitor created for the purpose of running the report.</li> <li>▶ We highly recommend that you deploy these monitors using the applicable solution templates for these monitors. The templates are preconfigured with the correct measurement counters and options already selected.</li> <li>▶ The Server-Centric report is not supported in Firefox 2.x.</li> <li>▶ If a monitor encounters a problem and returns non-applicable data, that data point is skipped. Thus, you may see missing data points in the graph.</li> </ul>
<b>Included in Tasks</b>	<p>“Create a Server-Centric Report – Workflow” on page 1883</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Generating a Server-Centric Report” on page 1881</li> <li>▶ “Create a Server-Centric Report – Scenario” on page 1885</li> </ul>

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	<p>Click to create a snapshot of the report you are viewing and highlight important areas of the report by drawing shapes, lines, and adding text to the snapshot. For details on the Annotation Tool user interface, see “Annotation Tool” on page 2085.</p>
	<p>Click to format the report data to a file for exporting. Select the format for the file. The options are printer-friendly, CSV, Excel, or XML.</p>
	<p>Click to export the report data in an email. Select the option for sending the file. The options are HTML mail, HTML attachment, or PDF.</p> <p><b>Note:</b> To use the export functionality, you must add the SiteScope machine to the trusted sites.</p>
	<p>Click to view the report one time frame earlier than the currently displayed time frame.</p> <p><b>Tooltip:</b> Back</p> <p><b>Example:</b> If the value of the <b>View</b> box is <b>Day</b>, clicking this button displays data for one day earlier than the currently displayed report.</p>
	<p>Click to view the report one time frame later than the currently displayed time frame.</p> <p><b>Tooltip:</b> Forward</p> <p><b>Example:</b> If the value of the <b>View</b> box is <b>Day</b>, clicking this button displays data for one day later than the currently displayed report.</p>
<p><b>View</b></p>	<p>Select a time range for which you want to view the report. Available time ranges include the following:</p> <ul style="list-style-type: none"> <li>▶ Custom (enables you to configure any range)</li> <li>▶ Hour, Day, Week</li> <li>▶ Past hour, Past day, Past week</li> </ul>

GUI Element	Description
<b>From/To &lt;date links&gt;</b>	<p>Click the <b>From</b> link to configure a start date and time for the report. Click the <b>To</b> link to configure an end date and time for the report. The calendar contains the following buttons:</p> <ul style="list-style-type: none"><li>▶ <b>OK.</b> Updates the date link for the selected date and closes the calendar.</li><li>▶ <b>Revert.</b> Returns to the previously selected report date.</li><li>▶ <b>Current.</b> Selects today's date in the calendar.</li><li>▶ <b>Cancel.</b> Closes the calendar without making any changes.</li></ul>
<b>Generate</b>	Click to create a report for the date range displayed in the date links.

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tooltip>	Hold the pointer over any data point on the graph to display a tooltip showing the value at the selected time of the utilization for the selected metric, as well as the date and time.
Server name	The name of the server appears above the Utilization graph.
Utilization graph	<p>A graph displaying utilization over time. The different colored lines represent CPU utilization, memory utilization, and network utilization. All three metrics are scaled as percents (that is, out of 100% utilization).</p> <p>You can click on a data point in the graph to focus in on a shorter timer range. The data tables are updated to show results for the time of the data point you selected (clicking any of the three data points for the same time updates the report in the same way). This is useful when you notice a point with particularly high utilization. By clicking on the point, you can determine the cause of the high utilization.</p> <p><b>Note:</b> Network utilization is supported for Windows servers only.</p>
Top 5 CPU Utilization Processes table	A table displaying the top five processes in terms of CPU utilization at any point in the graph. The table displays the process name and the CPU utilization value as a percent of total available CPU processing potential.
Top 5 Memory Consumption Processes table	A table displaying the top five processes in terms of memory consumption at any point in the graph. The table displays the process name and the memory consumption value in kilobytes.

## SiteScope Server Health

This chapter includes the main concepts, tasks, and reference information for monitoring SiteScope server health.

### **This chapter includes:**

#### Concepts

- ▶ SiteScope Health Overview on page 1896
- ▶ SiteScope Health Group on page 1899
- ▶ BAC Integration Configuration Monitor on page 1900
- ▶ BAC Integration Statistics Monitor on page 1901
- ▶ SiteScope Log Events Monitor on page 1901
- ▶ SiteScope Monitor Load Monitor on page 1902
- ▶ SiteScope Server Health Monitor on page 1902

#### Tasks

- ▶ Analyze SiteScope Health Monitor Data on page 1903

#### Reference

- ▶ SiteScope Health User Interface on page 1906

## SiteScope Health Overview

SiteScope Health is a specially designed group of monitors that display information about SiteScope's the performance and availability SiteScope itself. Health monitors retrieve data about SiteScope's resource usage, key processes, monitor load, server parameters, and the integrity of key configuration files.

By default, the daily monitor logs record the SiteScope Health monitoring data and let you can create reports on SiteScope's performance and operational health. These log files are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions. For example, SiteScope's audit log contains configuration changes performed in the new user interface, such as creation of monitors, templates, alerts, and so forth.

Together with the SiteScope Health monitoring, the SiteScope Progress Report provides several key indicators you use to monitor the performance of the SiteScope application.

This section includes the following topics:

- “Skipped Monitor Events” on page 1897
- “Problems Reporting Data” on page 1898



## Skipped Monitor Events

A SiteScope monitor is reported as skipped if the monitor fails to complete its actions before it is scheduled to run again. This can occur with monitors that have complex actions to perform, such as querying databases, stepping through multi-page URL sequences, waiting for scripts to run, or waiting for an application that has hung.

For example, assume you have a URL Sequence Monitor that is configured to transit a series of eight Web pages. This sequence includes performing a search which may have a slow response time. The monitor is set to run once every 60 seconds. When the system is responding well, the monitor can run to completion in 45 seconds. However, at times, the search request takes longer and then it takes up to 90 seconds to complete the transaction. In this case, the monitor has not completed before SiteScope is scheduled to run the monitor again. SiteScope detects this and makes a log event in the SiteScope error log. The SiteScope Log Event Monitor detects this and signals an error status.

A monitor may also skip if it is a monitor type that requires a process from the process pool but the process pool limit has been reached. Generally, this is not likely to happen but may occur in some situations with high monitoring load. The SiteScope Health Log Event Monitor also watches for process pool events. Skipped monitors can cause loss of data when a monitor run is suspended due because a previous run has not completed or has become hung by a unresponsive application. They can also cause SiteScope to automatically stop and restart itself, an event that is also monitored by the SiteScope Health Log Event Monitor. A restart is done in an effort to clear problems and reset monitors. However, this can also lead to gaps in monitoring coverage and data. Adjusting the run frequency at which a monitor is set to run or specifying an applicable timeout value can often correct the problem of skipping monitors.

**Note:**

- ▶ You can enable a setting that automatically disables monitors that exceed the maximum allowed skip count. If this occurs, SiteScope shuts down with an error and sends an email to the SiteScope administrator about the skipping monitor to signal the disable event. To enable this setting: In the preferences view, click **Infrastructure Preferences**, and expand the **Server Settings** panel. Select the **Shutdown on monitor skips** check box. This functionality is disabled by default.
  - ▶ You can control the maximum number of processes available. You should only change this setting if adjustments to monitor configurations do not resolve the monitor performance problems. The initial value is 200 processes per pool (by default, the maximum processes per pool is 20). To change this setting: In the preferences view, click **Infrastructure Preferences**, and expand the **General Settings** panel. Configure the number of processes in the **Maximum processes per pool** box.
- 

## **Problems Reporting Data**

SiteScope Health monitors are also configured to report events that indicate a problem with the transfer of SiteScope monitor and configuration data to an HP Business Availability Center installation. For information about troubleshooting data reporting to Business Availability Center, see “Troubleshooting and Limitations” on page 170.

## SiteScope Health Group

SiteScope Health monitors can monitor several key aspects of its own environment to help uncover monitor configuration problems as well as SiteScope server load. SiteScope can also monitor its connectivity and related data events when connected to HP Business Availability Center.

Similar to regular monitors, Health monitors can be edited in order to reconfigure their frequency and thresholds. Administrators can enhance the Health group by adding new monitors targeting additional servers and environments.

The Health monitor group is displayed as a health icon within the main SiteScope container. You view the contents of the Health monitor group by clicking the **Health** container.

SiteScope Health monitoring includes the following monitor types:

Monitor Type	Default Name	Description
BAC Integration Configuration Monitor	BAC Integration Configuration	Checks the correctness of the configuration between SiteScope and Business Availability Center when SiteScope is configured as a data collector for HP Business Availability Center.
BAC Integration Statistics Monitor	BAC Integration Statistics	Checks the traffic volume between SiteScope and Business Availability Center when SiteScope is configured as a data collector for HP Business Availability Center.
Log Event Health Monitor	Log Event Checker	Checks for certain events logged to the SiteScope error log.
Monitor Load Monitor	Monitor Load Checker	Checks for data about the number of monitors being run or waiting to run.

Monitor Type	Default Name	Description
Health of SiteScope Server Monitor	Health of SiteScope Server	Checks a large number of server process and resources for the server on which SiteScope is running.
SSL Certificates State Monitor	SSL Certificates State	Checks the state of SSL certificates in the default keystore.

## BAC Integration Configuration Monitor

When SiteScope is integrated as a data collector for Business Availability Center, this health monitor enables you to track the correctness of SiteScope's integration with the Business Availability Center configuration. This monitor is useful for viewing the number of groups, monitors, and measurements reporting to Business Availability Center that have an invalid path, internal name, or ID. It also displays the number of duplicate Topaz IDs, and instances where the Topaz ID is (-1).

This section also includes:

- ▶ “Troubleshooting and Limitations” on page 1900
- ▶ “Configuring the Monitor” on page 1901

### Troubleshooting and Limitations

- ▶ If there are objects with duplicate BAC IDs or with BAC ID == (-1):
  - ▶ Open a JMX Console (there is one provided in <SiteScope root directory>\java\bin\jconsole.exe), and enter 26767 in the **Port** field.
  - ▶ In the **MBeans** tab, select **com.mercury.sitescope/Integration/Bac/Tools/BacIntegrationToolsJMX**.
    - ▶ For objects with duplicate BAC IDs, activate `fixDuplicateBACConfiguration()`.
    - ▶ For objects with BAC ID == (-1), activate `fixMinusOneBACConfiguration()`.

- It is also recommended to activate `softSync()` to send the new configuration to Business Availability Center.
- If measurements have the wrong category ID, you should restart SiteScope.

## Configuring the Monitor

For details on configuring the monitor, see “BAC Integration Configuration Monitor Page” on page 1907.

## BAC Integration Statistics Monitor

The BAC Integration Statistics monitor checks the health of HP Business Availability Center. When SiteScope is integrated as a data collector for Business Availability Center, this health monitor enables you to track the volume of traffic between SiteScope and Business Availability Center. SiteScope sends metrics to BAC every minutes.

For details on configuring the monitor, see “BAC Integration Statistics Monitor Page” on page 1909.

## SiteScope Log Events Monitor

The Log Event Monitor is the equivalent of a SiteScope monitor group that watches the SiteScope Error Log (**error.log**) for certain events. These events include Log entries indicating that a monitor has been skipped or there was a problem in reporting data to another application.

For details on configuring the monitor, see “Log Event Health Monitor Page” on page 1910.

## SiteScope Monitor Load Monitor

The Monitor Load Monitor watches how many monitors are running and how many are waiting to be run. Watching monitor load is important to help maintain monitoring performance and continuity. If the number of monitors waiting approaches or exceeds the number of monitors running, adjustments should be made to monitor configurations to reduce the number of monitors waiting to run. Generally, this can be done by reducing the run frequency of some monitors.

For details on configuring the monitor, see “Monitor Load Monitor Page” on page 1913.

## SiteScope Server Health Monitor

The Health of SiteScope Server Monitor is the equivalent of a SiteScope monitor that monitors server resources on the server where SiteScope is running. This includes monitors for CPU, disk space, memory, and key processes. A problem with resource usage on the SiteScope server may be caused by monitors with configuration problems or may simply indicate that a particular SiteScope is reaching its performance capacity. For example, high CPU usage by SiteScope may indicate that the total number of monitors being run is reaching a limit. High disk space usage may indicate that the SiteScope monitor data logs are about to exceed the capacity of the local disk drives. For details on SiteScope data logging options, see “Log Preferences” on page 1449.

---

**Note:** This monitor is supported in SiteScopes that are running on Windows versions only. However, this monitor can monitor remote servers running on any platform/operating system.

---

For details on configuring the monitor, see “Health of SiteScope Server Monitor Page” on page 1914.

## Analyze SiteScope Health Monitor Data

This task describes the steps involved in analyzing SiteScope Health monitor data and viewing the SiteScope log files and server statistics.

This task includes the following steps:

- “Prerequisites” on page 1903
- “Deploy SiteScope Health Monitors” on page 1903
- “View SiteScope Health Monitors” on page 1904
- “View SiteScope Log Files” on page 1905
- “View Monitor Performance Data” on page 1905

### 1 Prerequisites

To access the log files and the Progress Report, you must have the correct user privileges.

- a** In the left pane, click **Preferences** and select **User Management**.
- b** Right-click the user name, and select **Edit User**.
- c** In the Edit User dialog box, expand **Permissions**.
- d** In the **Other** section, make sure that **View server statistics** and **View logs** are selected (these settings are selected by default).

### 2 Deploy SiteScope Health Monitors

If the SiteScope Health monitors are not present when you import a SiteScope to System Availability Management in HP Business Availability Center, you must deploy the monitors.

For details on how to perform this task, see “Deploy SiteScope Health Monitors” on page 1906.

---

**Note:** The SiteScope health monitors are normally present, because they are enabled automatically when SiteScope is deployed.

---

### 3 View SiteScope Health Monitors

You can view the data collected by the SiteScope Health monitors in the SiteScope Dashboard.

For details on the user interface, see “SiteScope Health User Interface” on page 1906.

#### Example

Show Child Groups and Monitors	Status	Type	Target	Summary	Updated	Description			
Selected node									
Health		Group		6 in group, ...	6/28/09 1:...				
Groups (0 out of 0)									
Monitors (6 out of 6)									
BAC Integration Configuration		BACIntegr...	787x203	"Site Scope...	6/28/09 4:...				
BAC Integration Statistics		BAC Integr...		Currently I...	6/28/09 1:...				
Health of SiteScope Server		Monitor Lo...	SiteScope ...	{ Threshol...	6/28/09 1:...				
Log Event Checker		Log Event ...		*skipped #...	6/28/09 1:...				
Monitor Load Checker		Monitor Load		Current M...	6/28/09 1:...				
SSL Certificates State		SSLCertific...		Expired ce...	6/28/09 4:...				



## 4 View SiteScope Log Files

You can view the various SiteScope log files in the Log Files page in the Server Statistics context. For details on the user interface, see “Log Files Page” on page 1954.

### Example

Type	Log File	Size	Last Modified
Audit Logs	<a href="#">audit.log</a>	83 K	11/06/2008 10:42:03
BAC Integration Logs	<a href="#">bac_integration.log</a>	116 bytes	11/06/2008 07:23:17
Daily Logs	<a href="#">SiteScope2008_11_06.log</a>	878 K	11/06/2008 10:44:38
Error Logs	<a href="#">error.log</a>	468 K	11/06/2008 10:36:00
Other Logs	<a href="#">access.log</a>	428 bytes	11/06/2008 10:19:23
Other Logs	<a href="#">alert.log</a>	9 K	11/06/2008 05:45:10
Other Logs	<a href="#">auto_sanity.log</a>	524 K	11/06/2008 10:25:49
Other Logs	<a href="#">baselining.log</a>	0 bytes	11/06/2008 05:33:50
Other Logs	<a href="#">data_integration.log</a>	0 bytes	11/06/2008 05:33:50
Other Logs	<a href="#">jmdrv.log</a>	0 bytes	11/06/2008 05:43:11
Other Logs	<a href="#">LinkReport_Basic7.log</a>	186 bytes	11/06/2008 10:43:18
Other Logs	<a href="#">mdrv.log</a>	0 bytes	11/06/2008 05:43:11
Other Logs	<a href="#">mirror.log</a>	0 bytes	11/06/2008 05:33:50
Other Logs	<a href="#">monitorCount.log</a>	907 bytes	11/06/2008 10:35:42
Other Logs	<a href="#">quota_control.log</a>	0 bytes	11/06/2008 05:33:50
Other Logs	<a href="#">request_statistics.log</a>	16 K	11/06/2008 05:33:50
Other Logs	<a href="#">statisticsLogger.log</a>	40 K	11/06/2008 10:44:09
Other Logs	<a href="#">template_persistency_upg...</a>	527 K	11/06/2008 06:47:26
Run Monitor Logs	<a href="#">RunMonitor.log</a>	152 K	11/06/2008 09:16:38

## 5 View Monitor Performance Data

You can view the load on the SiteScope server and a list of the most recently run monitors in the Server Statistics context.

For more details on this topic, see “Viewing Server Statistics” on page 1921.

## **Deploy SiteScope Health Monitors**

This task describes how to deploy SiteScope Health monitors to a SiteScope installation if the monitors were not present when you imported a SiteScope to System Availability Management in HP Business Availability Center.

### **To deploy SiteScope Health Monitors:**

- 1** Open the SiteScope container to which you want to display the Health monitors. Confirm that the SiteScope includes the Health monitor group container.

---

**Note:** The Health monitor group container is identified with a health indicator icon.

---

- 2** Find the **Health Templates** in the monitor tree. Click to expand the container contents. The available Health monitor templates are displayed.
- 3** Select the Health monitor template for the operating system on which the SiteScope you want to monitor is running. The choices are:
  - UNIX Health Monitors
  - Windows Health Monitors
- 4** Right-click the template icon and select **Copy** from the action menu.
- 5** Right-click the **Health** monitor group container of the SiteScope to which you want to deploy the Health monitors and select **Paste**. The monitors in the selected template are then configured and deployed to the selected SiteScope server.

## **SiteScope Health User Interface**

### **This section includes:**

- BAC Integration Configuration Monitor Page on page 1907
- BAC Integration Statistics Monitor Page on page 1909

- Log Event Health Monitor Page on page 1910
- Monitor Load Monitor Page on page 1913
- Health of SiteScope Server Monitor Page on page 1914
- SSL Certificates State Monitor Page on page 1919

## BAC Integration Configuration Monitor Page

<b>Description</b>	Enables you to check the correctness of SiteScope's integration with the Business Availability Center configuration.  <b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, expand <b>Health</b> and click <b>BAC Integration Configuration</b> .
<b>Important Information</b>	Monitor data is relevant only if SiteScope is integrated as a data collector for Business Availability Center.
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “BAC Integration Configuration Monitor” on page 1900</li> <li>➤ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Counters</b>	
<b>Total Groups.</b>	The total number of groups reporting data to Business Availability Center.
<b>Total Monitors</b>	The total number of monitors reporting data to Business Availability Center.

GUI Element	Description
<b>Duplicate BAC ID</b>	The number of duplicate BAC IDs reported to Business Availability Center. Every SiteScope object has a unique BAC ID. If two objects have the same ID, only one of these objects can send its data to Business Availability Center. For troubleshooting on this subject, see “Troubleshooting and Limitations” on page 1900.
<b>BAC ID == (-1)</b>	Every SiteScope object has a unique BAC ID. If the ID value for a SiteScope object is (-1), SiteScope does not send its data to Business Availability Center. For troubleshooting on this subject, see “Troubleshooting and Limitations” on page 1900.
<b>Group with invalid path</b>	If the SiteScope group does not have a valid path, SiteScope does not send the group to Business Availability Center.
<b>Groups with duplicate name</b>	If the SiteScope group does not have a unique internal name, SiteScope does not send the group to Business Availability Center.
<b>Monitor with invalid path</b>	If the SiteScope monitor does not have a valid path, SiteScope does not send the monitor to Business Availability Center.
<b>Monitors without internal ID</b>	If the SiteScope monitor does not contain a unique internal ID, SiteScope does not send the monitor to Business Availability Center.
<b>Monitors without internal name</b>	If the SiteScope monitor does not contain a valid internal name, SiteScope does not send this monitor to Business Availability Center.
<b>Measurements with wrong category ID</b>	If SiteScope measurements do not contain a valid category ID, SiteScope does not send the measurements to Business Availability Center. For troubleshooting on this subject, see “Troubleshooting and Limitations” on page 1900.
<b>Target with BAC ID == (-1)</b>	Every remote target has a unique BAC ID. If the ID value is (-1), SiteScope does not send its data to Business Availability Center. For troubleshooting on this subject, see “Troubleshooting and Limitations” on page 1900.

## BAC Integration Statistics Monitor Page

<b>Description</b>	Enables you to check the volume of traffic between SiteScope and HP Business Availability Center. <b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, expand <b>Health</b> and click <b>BAC Integration Statistics</b> .
<b>Important Information</b>	Monitor data is relevant only if SiteScope is integrated as a data collector for Business Availability Center.
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “BAC Integration Configuration Monitor” on page 1900</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### Main Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Counters</b>	<ul style="list-style-type: none"> <li>▶ <b>Currently Logging to Business Availability Center.</b> Shows the amount of metrics currently logging per minute to Business Availability Center.</li> <li>▶ <b>Number of Topology Scripts in Queue.</b> Displays the number of Jython scripts waiting to be run. These scripts forward topology data to Business Availability Center and must be run whenever there is a configuration change in SiteScope. The queue can grow when a SiteScope is first registered to Business Availability Center or when there are many configuration changes made in the SiteScope.</li> </ul>

 **Log Event Health Monitor Page**

<b>Description</b>	<p>Enables you to monitor the local SiteScope installation <b>error.log</b> file for certain events. These events include log entries indicating that a monitor has been skipped or there was a problem in reporting data to another application.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, expand <b>Health</b> and click <b>Log Event Checker</b>.</p>
<b>Included in Tasks</b>	“Analyze SiteScope Health Monitor Data” on page 1903
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Log Events Monitor” on page 1901</li> <li>➤ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Log Event Health Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Counters	<ul style="list-style-type: none"> <li>➤ <b>skipped #1.</b> A monitor has skipped its scheduled run once.</li> <li>➤ <b>skipped #2.</b> A monitor has skipped its scheduled run two times.</li> <li>➤ <b>skipped #3.</b> A monitor has skipped its scheduled run three times.</li> <li>➤ <b>skipped #4.</b> A monitor has skipped its scheduled run four times.</li> <li>➤ <b>skipped #5.</b> A monitor has skipped its scheduled run five times.</li> <li>➤ <b>SiteScope is shutting down.</b> SiteScope has been shut down.</li> <li>➤ <b>Reached the limit of processes in the process pool.</b> The number of processes requested from the process pool exceeds the number of processes available in the pool.</li> <li>➤ <b>Error. data reporter failed to report chunk of data.</b> There was a fault in the transfer of SiteScope monitor measurement data to HP Business Availability Center.</li> <li>➤ <b>Error. config reporter failed to report chunk of data.</b> There was a fault in the transfer of SiteScope configuration data to HP Business Availability Center System Availability Management.</li> <li>➤ <b>Error. HP Business Availability Center failed to process data.</b> HP Business Availability Center reported a fault in processing data sent from SiteScope.</li> </ul>

GUI Element	Description
<p><b>Counters</b></p>	<ul style="list-style-type: none"> <li>➤ <b>Error. CacheSender. Got to the max number of cached files.</b> SiteScope has reached the maximum number of cached data file awaiting transfer to HP Business Availability Center. This may occur if data transfer between SiteScope and HP Business Availability Center has been interrupted.</li> <li>➤ <b>Error. CacheSender. Got to the max old dir size.</b> SiteScope has reached the maximum directory size for cached data file awaiting transfer to HP Business Availability Center. This may occur if data transfer between SiteScope and HP Business Availability Center has been interrupted.</li> <li>➤ <b>HP Business Availability Center SEVERE.</b> HP Business Availability Center reported a data transfer or processing fault with a status of SEVERE.</li> <li>➤ <b>Commit verification failed.</b></li> <li>➤ <b>Error loading monitor.</b></li> <li>➤ <b>Error contacting mirror server.</b></li> <li>➤ <b>Error: open SSH connections limit reached.</b></li> <li>➤ <b>Error: failure in baseline process.</b></li> <li>➤ <b>Error: failed to parse rule.</b></li> <li>➤ <b>Topology Reporter failed to report.</b></li> </ul>
<p><b>Reset counter values</b></p>	<p>Click to reset the monitor counter values to 0.</p>



## Monitor Load Monitor Page

<b>Description</b>	Enables you to check several SiteScope load statistics reported by the Progress Report for the local SiteScope installation.  <b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, expand <b>Health</b> and click <b>Monitor Load Checker</b> .
<b>Included in Tasks</b>	“Analyze SiteScope Health Monitor Data” on page 1903
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Monitor Load Monitor” on page 1902</li> <li>➤ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### Monitor Load Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Counters</b>	<ul style="list-style-type: none"> <li>➤ Current Monitors Run Per Minute</li> <li>➤ Current Monitors Running</li> <li>➤ Current Monitors Waiting</li> <li>➤ Maximum Monitors Run Per Minute</li> <li>➤ Maximum Monitors Running</li> <li>➤ Maximum Monitors Waiting</li> </ul>

## Health of SiteScope Server Monitor Page

<b>Description</b>	<p>Enables you to check the SiteScope server resource and process statistics for the local SiteScope installation.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, expand <b>Health</b> and click <b>Health of SiteScope Server</b>.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ Process/perfex counters were removed from the SiteScope Server Health monitor and are no longer supported.</li> <li>▶ <b>Note when working in template mode:</b> The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.</li> </ul>
<b>Included in Tasks</b>	<p>“Analyze SiteScope Health Monitor Data” on page 1903</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Server Health Monitor” on page 1902</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

## Health of SiteScope Server Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Counters (on UNIX)</b>	<ul style="list-style-type: none"> <li>➤ Current Monitors Run Per Minute</li> <li>➤ Current Monitors Running</li> <li>➤ Current Monitors Waiting</li> <li>➤ Maximum Monitors Run Per Minute</li> <li>➤ Maximum Monitors Running</li> <li>➤ Maximum Monitors Waiting</li> <li>➤ Used Disk Space on SiteScope Drive (accessible on SiteScope installed on UNIX)</li> <li>➤ MegaBytes Available on SiteScope Drive</li> <li>➤ Physical Memory Free</li> <li>➤ Physical Memory Free Megabytes</li> <li>➤ Swap Free</li> <li>➤ Swap Free Megabytes</li> <li>➤ Load Avg 5min</li> <li>➤ SiteScope Process Memory</li> <li>➤ SiteScope Process Thread Count</li> <li>➤ SiteScope Process Handle Count</li> <li>➤ Average CPU</li> <li>➤ PageIns/sec</li> <li>➤ PageOuts/sec</li> <li>➤ SwapIns/sec</li> <li>➤ SwapOuts/sec</li> <li>➤ ContextSwitches/sec</li> <li>➤ Net_TotalPacketsIn/sec</li> <li>➤ Net_TotalPacketsOut/sec</li> <li>➤ Net_TotalCollisions/sec</li> </ul>

GUI Element	Description
<p><b>Counters (on Windows)</b></p>	<p><b>Memory</b></p> <ul style="list-style-type: none"> <li>➤ Page Faults/sec</li> <li>➤ Pool Paged Bytes</li> <li>➤ Pool Nonpaged Bytes</li> <li>➤ % Committed Bytes In Use</li> <li>➤ Available MBytes</li> </ul> <p><b>System</b></p> <ul style="list-style-type: none"> <li>➤ Context Switches/sec</li> <li>➤ File Data Operations/sec</li> <li>➤ System Up Time</li> <li>➤ Processor Queue Length</li> <li>➤ Processes</li> <li>➤ Threads</li> </ul> <p><b>Processor</b></p> <ul style="list-style-type: none"> <li>➤ _Total <ul style="list-style-type: none"> <li>➤ % Processor Time</li> <li>➤ % DPC Time</li> </ul> </li> </ul> <p><b>Process</b></p> <ul style="list-style-type: none"> <li>➤ java <ul style="list-style-type: none"> <li>➤ Thread Count</li> <li>➤ Pool Paged Bytes</li> <li>➤ Pool Nonpaged Bytes</li> <li>➤ Handle Count</li> </ul> </li> </ul>

GUI Element	Description
Counters (on Windows)	<p><b>Network Interface</b></p> <ul style="list-style-type: none"> <li>➤ MS TCP Loopback interface <ul style="list-style-type: none"> <li>➤ Bytes Total/sec</li> <li>➤ Current Bandwidth</li> <li>➤ Bytes Received/sec</li> <li>➤ Bytes Sent/sec</li> <li>➤ &lt;Ethernet_hardware&gt; (hardware specific to the particular SiteScope server)</li> <li>➤ Bytes Total/sec</li> <li>➤ Current Bandwidth</li> <li>➤ Bytes Received/sec</li> <li>➤ Bytes Sent/sec</li> </ul> </li> </ul> <p><b>LogicalDisk</b></p> <ul style="list-style-type: none"> <li>➤ &lt;logical_drive&gt; (hardware specific to the particular SiteScope server) <ul style="list-style-type: none"> <li>➤ % Free Space</li> <li>➤ Free Megabytes</li> <li>➤ Avg. Disk Bytes/Transfer</li> </ul> </li> <li>➤ _Total <ul style="list-style-type: none"> <li>➤ % Free Space</li> <li>➤ Free Megabytes</li> <li>➤ Avg. Disk Bytes/Transfer</li> </ul> </li> </ul> <p><b>PhysicalDisk</b></p> <ul style="list-style-type: none"> <li>➤ _Total <ul style="list-style-type: none"> <li>➤ Current Disk Queue Length</li> <li>➤ Disk Transfers/sec</li> </ul> </li> <li>➤ &lt;physical_disk(s)&gt; (hardware specific to the particular SiteScope server) <ul style="list-style-type: none"> <li>➤ Current Disk Queue Length</li> <li>➤ Disk Transfers/sec</li> </ul> </li> </ul>

GUI Element	Description
Counters (on Windows)	<b>Server</b> <ul style="list-style-type: none"><li>▶ Bytes Total/sec</li><li>▶ Errors Logon</li><li>▶ Errors Access Permissions</li><li>▶ Errors System</li><li>▶ Files Open</li><li>▶ Server Sessions</li></ul>

## SSL Certificates State Monitor Page

<b>Description</b>	<p>Enables you to check the state of SSL certificates in the default keystore (&lt;SiteScope root directory&gt;\java\lib\security\cacerts). This is where client certificates that are imported for monitoring URL, WebSphere Application Server, or VMware-based servers are stored.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, expand <b>Health</b> and click <b>SSL Certificates State</b>.</p>
<b>Included in Tasks</b>	“Analyze SiteScope Health Monitor Data” on page 1903
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Certificate Management” on page 1535</li> <li>▶ The monitor specific settings are described below. For details on the settings common to all monitors, see “Common Monitor Settings” on page 354.</li> </ul>

### SSL Certificates State Monitor Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Days before expiration</b>	<p>If a certificate is due to expire within the specified number of days (but has not yet expired), it is added to the <b>Certificates expiring soon</b> counter.</p> <p><b>Default value:</b> 7 days</p>
<b>Counters</b>	<ul style="list-style-type: none"> <li>▶ Expired certificates. Comma-separated list of already expired certificates</li> <li>▶ Certificates expiring soon. Comma-separated list of certificates that are due to expire within the period specified in Days before expiration. soon (fasted that N days, determined by monitor settings), but not expired yet.</li> <li>▶ Number of expired certificates</li> <li>▶ Number of certificates expiring soon</li> </ul>





# 155

---

## Viewing Server Statistics

This chapter includes the main concepts, tasks, and reference information for viewing SiteScope server statistics.

### **This chapter includes:**

#### **Concepts**

- ▶ Using Server Statistics on page 1922
- ▶ Interpreting SiteScope Server Load Statistics on page 1923
- ▶ Using Log Files on page 1927

#### **Tasks**

- ▶ Analyze SiteScope Server Statistics on page 1930
- ▶ Configure the Audit Log on page 1931

#### **Reference**

- ▶ SiteScope Log File Columns on page 1932
- ▶ Audit Log Entries on page 1933
- ▶ SiteScope Server Statistics User Interface on page 1943

## Using Server Statistics

The SiteScope **Server Statistics** context provides an overview of several key SiteScope server performance metrics that can be used for analyzing SiteScope performance, stability, health, and for debugging bottlenecks. It includes statistics that show load on the SiteScope server, a list of running monitors and the most recently run monitors, perfex pool summary, thread pools, Telnet connections, and SSH connections. It also displays the SiteScope log files. The Server Statistics context is updated every 20 seconds.

The Server Statistics context includes the following pages:

Page	Description
<b>General</b>	Displays key SiteScope server load statistics, including the number of monitors running and waiting, and a list of running monitors by type. For details of the user interface, see “General Page” on page 1944.
<b>Running Monitors</b>	Displays a list of which SiteScope monitors are running, and which monitors have run recently, at what time, and what was the returned status. For details of the user interface, see “Running Monitors Page” on page 1945.
<b>Perfex Process Pool</b>	Displays a process manager summary, and statistics tables for the perfex and perfex_dispatcher pools. For details of the user interface, see “Perfex Process Pool Page” on page 1947.
<b>SSH Connections</b>	Displays SSH statistics and SSH connection summary when using SSH to connect to remote UNIX or Windows servers. For details of the user interface, see “SSH Connections Page” on page 1950.

Page	Description
<b>Telnet Connections</b>	Displays telnet statistics when using telnet to connect to remote UNIX or Windows servers. For details of the user interface, see “Telnet Connections Page” on page 1952.
<b>Log Files</b>	Displays the list of log files in SiteScope that are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions. For details of the user interface, see “Log Files Page” on page 1954.

## Interpreting SiteScope Server Load Statistics

Monitoring Load can be a key indicator of SiteScope scaling problems, monitor configuration problems, or network performance issues. The following is a brief explanation of the SiteScope monitor execution model and interpreting the server performance data in the context of this model.

A SiteScope monitor instance is essential as an instruction set that is run by the SiteScope application on a regularly scheduled interval. While a monitor instance is defined, SiteScope queues the monitor for execution based on the run (update) frequency and schedule options. If the monitor instance is marked as disabled, it is still scheduled in the queue but the normal instructions are not run.

As a Java-based application, SiteScope makes use of multi-threading to accomplish parallel execution of monitor tasks. Each monitor instance scheduled for execution is assigned a thread. Once it is assigned a thread, the monitor instance becomes a **Monitor Running**. It remains bound to the thread until the monitor execution instruction has either received a result or the timeout value, if applicable, has been reached.

Even in this model, monitor execution is not instantaneous and there is a finite limit to the number of monitor threads that can be run in parallel. If not more threads are available, a monitor that is queued for execution becomes a **Monitor Waiting** for an execution thread.

It is difficult to assign specific values and limits to SiteScope Monitoring Load because the specifics of the server capacity and network deployment can vary widely. The monitoring load may also vary significantly over time simply due to transient network traffic issues or SiteScope monitor configuration problems.

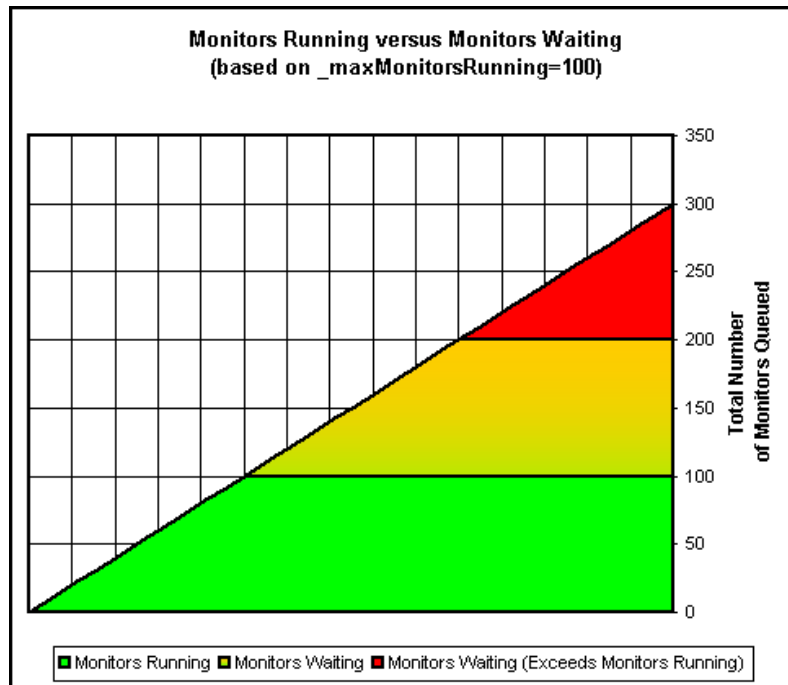
One key warning signal for interpreting monitoring load is the ratio of Monitors Waiting to Monitors Running. Generally, having some monitors waiting for execution is not a problem unless the ratio of Monitors Waiting to Monitors Running is consistently 1:2 or higher. For example, if the number of monitors running is at the maximum of 100 and there are 50 monitors waiting, this represents a ratio of 1 monitor waiting for every two running.

---

**Note:** The initial maximum number of monitor execution threads for the `_maxMonitorsRunning=` setting controlled by the `master.config` file is 400 (the default value is 30 in `master.xml`).

---

The graph below presents a visualization of the relationship between Monitors Running and Monitors Waiting. This graph is based on the `_maxMonitorsRunning` setting of 100 monitors. The green region shows that SiteScope is able to run all queued monitors until the number of queued monitors exceeds 100. At that level, additional monitors that are scheduled to run are given the status of Monitor Waiting. The red region represents an area where the number of monitors waiting is more than twice the number of monitors running. This is a certain indication that your SiteScope monitor configurations are not well aligned with the capacity of the server and network.



You can adjust the following monitor configuration settings if there are consistently too many monitors waiting:

- ▶ **Frequency.** This is the basic schedule parameter for every monitor type. A large number of Monitors Running and Monitors Waiting can often be explained by a large number of monitors set to run (or update) at short intervals. The minimum update interval is 15 seconds. Depending on a number of system factors, there are several monitor actions which may take more than 15 seconds to complete. For example, Web transactions, database queries, logging onto remote servers, and some regular expression matches may delay monitor completion. Use the “Monitor Summary Report” on page 2080 to check the **Frequency** setting for groups of monitors and consider increasing the value for some monitors.
- ▶ **Verify error.** Regular or extensive use of this option has the effect of rapidly increasing the monitor run queue whenever the applicable SiteScope monitors detect an error condition. While this option has its purpose, it should not be used by default on every monitor. Use the “Monitor Summary Report” on page 2080 to list monitors that may have the **Verify error** setting enabled.

For details on SiteScope server performance data, see “Running Monitors Page” on page 1945.

## Using Log Files

SiteScope maintains a number of log files that are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions.

Log files can be accessed using the Log File menu in the Server Statistics context. When you click a log file, a new browser window opens displaying the text of the log file. You can use the scroll bars to view the contents of the log or use the browser's text Find utility to locate specific information. For example, you can search for a unique text string that appears in a monitor's **Name** property to locate entries for a particular monitor instance. For details on the various SiteScope log files, see "Log Files Page" on page 1954.

The log files are written in plain text and stored in the `<SiteScope_root_path>\logs` directory. In the default configuration, these log files are tab-delimited text files. Understanding the order and content of these files is useful for examining particular monitor results or for porting the SiteScope monitor results to another database. For details, see "SiteScope Log File Columns" on page 1932.

This section also includes:

- "Using the Audit Log" on page 1928
- "Audit Log Limitations" on page 1929

## Using the Audit Log

SiteScope's audit log provides you with a record of actions performed in SiteScope, the time they were performed, and by whom. It contains configuration changes performed in the new user interface, such as creation of monitors, templates, alerts, and so forth.

---

**Note:** When SiteScope is attached to System Availability Management Administration in HP Business Availability Center, the actions you perform on SiteScope appear in HP Business Availability Center's audit log and not in SiteScope's audit log.

---

As each operation is performed, an entry is made in the audit log. When the current audit log reaches its size limit, it is closed and a new log is created. Older logs are named `audit.log.1`, `audit.log.2`, and so forth. The higher the number concatenated to the name, the older the log. For details on setting the size limit and the maximum number of backup audit logs to be kept, see "Configure the Audit Log" on page 1931.

The name of the current audit log is **audit.log** and it is found in the `<SiteScope root directory>\logs` directory. You can access the audit log from the directory or through the SiteScope application. For details on viewing the audit log, see "Log Files Page" on page 1954.

Most operations performed in the monitor tree are recorded in the audit log. For a list of operations that are not recorded in the audit log, see "Audit Log Limitations" on page 1929.



## Audit Log Limitations

- ▶ Audit log entries can be created only in English. This means that audit log entries are also displayed only in English, regardless of what language you use to view SiteScope.
- ▶ The following operations are not recorded in the audit log:
  - ▶ When a template is deployed, operations on the various elements in the template are not logged.

For example, you deployed a template that created group MM2\_Servers with monitors in the new group. The audit log entry is:

Operation performed: Configuration Template 'MM2' pasted on 'MM2\_Servers'.

Note that there are no entries in the audit log about creation of monitors in MM2\_Servers group.

- ▶ Attaching and detaching SiteScope to HP Business Availability Center are not logged.

When SiteScope is attached to System Availability Management Administration in HP Business Availability Center, the actions you perform on SiteScope appear in HP Business Availability Center's audit log and not in SiteScope's audit log.

- ▶ Group configurations that were made by using a <group name>.mg file are not recorded in the audit log. Only group changes made through the monitor tree are recorded in the audit log.

When you create a group in the monitor tree, a <group name>.mg file with all the configuration changes for the group is automatically created for that group. This means that you can configure a group through the monitor tree or by changing its mg file.

**Note:** SiteScope group .MG files are supported in SiteScope 10.10, however, the **Enable configuration files** option is no longer selected by default when SiteScope is installed. SiteScope group .MG files will be deprecated in SiteScope 11.00.

## Analyze SiteScope Server Statistics

This task describes the steps involved in analyzing SiteScope server statistics and log files.

This task includes the following steps:

- ▶ “Prerequisites” on page 1930
- ▶ “View SiteScope Server Statistics” on page 1930
- ▶ “View SiteScope Log Files” on page 1930

### 1 Prerequisites

To access the Server Statistics context, you must have the correct user privileges.

- a** In the left pane, click **Preferences** and select **User Management**.
- b** Right-click the user name, and select **Edit User**.
- c** In the Edit User dialog box, expand **Permissions**.
- d** In the **Other** section, make sure that **View server statistics** is selected (this settings is selected by default).

### 2 View SiteScope Server Statistics

You can view the load on the SiteScope server, a list of running and most recently run monitors, perfex process pool statistics, telnet connection statistics, and SSH connection statistics in the Server Statistics context.

For details on the user interface, see “SiteScope Server Statistics User Interface” on page 1943.

### 3 View SiteScope Log Files

You can view the various SiteScope log files in the Log Files page in the Server Statistics context. For details on the user interface, see “Log Files Page” on page 1954.

## Configure the Audit Log

This task describes the steps involved in configuring the maximum size of the audit log.

**To configure the audit log:**

- 1** Open the **log4j.properties** file located in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\** directory.
- 2** Set **MaxFileSize** to the maximum number of lines in the log.
- 3** Set **MaxBackupIndex** to the maximum number of backup audit logs to be kept before the oldest audit log is deleted.

For example, if **MaxBackupIndex** is 5, no more than 5 backup audit logs are kept. If 5 backup log files exist, then after the current **audit.log** file reaches **MaxFileSize** size, **audit.log.5** is deleted, **audit.log.4** is renamed to **audit.log.5**, **audit.log.3** to **audit.log.4** and so forth. The current **audit.log** is renamed **audit.log.1** and a new **audit.log** is created.

## SiteScope Log File Columns

When SiteScope runs a monitor instruction to test the availability of components in the infrastructure, the monitor results are written to data log files. The first six columns of each log entry in a SiteScope monitor data log are the same for each monitor type. After the first six columns of each log entry, the content of each column is specific for each monitor type.

The following table describes the content of these columns. The columns in each log file are written as tab-delimited text.

Column	Data in Column
1	Time and date the sample was recorded.
2	Category (for example, good, error, warning, nodata).
3	Monitor group name where the monitor defined (also called ownerID).
4	Monitor title text.
5	stateString (this is the status string that shows up on the Group details page).
6	id:sample number (a unique ID for this monitor where group + id is a unique key for a monitor). The sample number is a unique sample number for that monitor.

## Audit Log Entries

Each line of the audit log describes an operation performed in SiteScope.

This section includes the following topics:

- “SiteScope Startup” on page 1934
- “Group Operations” on page 1934
- “Monitor Operations” on page 1935
- “Update to General Preferences” on page 1935
- “Update to Other Preferences” on page 1936
- “Applying Templates” on page 1937
- “Template Containers” on page 1937
- “Create, Delete, Modify Templates” on page 1938
- “Template Variables” on page 1938
- “Template Groups” on page 1939
- “Template Remote Objects” on page 1939
- “Template Alerts” on page 1940
- “Template Monitors” on page 1940
- “Alerts” on page 1941
- “Reports” on page 1941
- “Global Search and Replace Operations” on page 1942
- “Login-Logout” on page 1942
- “Failed Login” on page 1942
- “Changed Password” on page 1943
- “Categories” on page 1943

## SiteScope Startup

When SiteScope is restarted, its entry is:

```
YYYY-MM-DD HH:MM:SS - SiteScope Audit Log initialized
```

## Group Operations

Operations performed on groups have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Group  
'<group_name>' '<operation>' '<container>'
```

where:

- **<group\_name>** is the name of the group that was operated on.
- **<operation>** can be one of the following:
  - **Created In.** The location where the group was created.
  - **Updated in.** The location where the group's information was updated.
  - **Deleted From.** The location from where the group was deleted.
  - **Pasted On.** The user copied information from one group to another.
- **<container>** is the name of the group container that was operated on.

## Monitor Operations

Operations performed on monitors have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Monitor
'<monitor_name>' '<operation>' '<container>'
```

- **<monitor\_name>** is the name of the monitor that was operated on.
- **<operation>** can be one of the following:
  - **Created In.** The location where the user created a monitor.
  - **Updated in.** The location from where the user updated a monitor's information.
  - **Deleted From.** The location where the user deleted a monitor.
  - **Pasted On.** The user copied information from one monitor to another.
- **<container>** is the name of the container.

## Update to General Preferences

Changes made in **General Preferences** under the **Preferences** container in the monitor tree have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed:
'<preferences_name>' updated
```

where **<preferences\_name>** is the name of the preference that was changed.

The nature of the change to the preference is not in the log.

## Update to Other Preferences

Changes to preferences other than those listed in **General Preferences** in the monitor tree have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed:  
'<preferences_name>' named '<object_name>' '<operation>'
```

- **<preferences\_name>** is the name of the preference.
- **<object\_name>** is the name of the object to which the preference refers.
- **<operation>** can be one of the following:
  - **Updated.** The user changed the preference.
  - **Deleted.** The user deleted the preference.

This format is used for the following types of preferences:

- Microsoft Windows Remote Servers
- UNIX Remote Servers
- Mail Preferences
- Pager Preferences
- SNMP Preferences
- Absolute Schedule Preferences
- Range Schedule Preferences
- User Preferences



## Applying Templates

When an entity is created by deploying a template, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Configuration
Template '<template_name>' pasted on '<group_name>'
```

- **<template\_name>** is the name of the template from which the entity was created.
- **<group\_name>** is the name of the group that contains the entity that was created from the template.

---

**Note:** To see which entities were created by deploying the template, look at the contents of template itself. Information about entities is not included in the audit log.

---

## Template Containers

When a template container is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
Container '<container_name>' '<operation>' '<container>'
```

- **<container\_name>** is the name of the template container that was either created, deleted, or updated.
- **<operation>** can be one of the following:
  - **Created in.** The location where the user created the template container.
  - **Deleted from.** The location from where the user deleted the template container.
  - **Updated in.** The location where the user changed the template container.
- **<container>** is the name of the container containing the template.

## Create, Delete, Modify Templates

When a template is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template  
'<template_name>' '<operation>' '<container>'
```

- ▶ **<template\_name>** is the name of the template that was either created, deleted, or updated.
- ▶ **<operation>** can be one of the following:
  - ▶ **Created in.** The location where the user created the template.
  - ▶ **Deleted from.** The location from where the user deleted the template.
  - ▶ **Updated in.** The location where the user changed the template.
- ▶ **<container>** is the name of the container containing the template.

## Template Variables

When a template variable related to an object, such as server ID, is created, deleted, or updated in a container, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template  
Variable '<variable_name>' '<operation>' '<container>'
```

- ▶ **<variable\_name>** is the name of the variable that was either created, deleted, or updated.
- ▶ **<operation>** can be one of the following:
  - ▶ **Created in.** The location where the template variable for the object was created.
  - ▶ **Deleted from.** The location where the template variable for the object was deleted.
  - ▶ **Updated in.** The location where the template variable for the object was updated.
- ▶ **<container>** is the name of the container containing the template variable.

## Template Groups

When a template group for a specific type of object is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template Group
'<group_name>' '<operation>' '<container>'
```

- **<group\_name>** is the name of the template group created, updated or deleted.
- **<operation>** can be one of the following:
  - **Created in.** The location where the template group for the object was created.
  - **Deleted from.** The location from where the template group for the object was deleted.
  - **Updated in.** The location where template for the object was updated.
- **<container>** is the name of the container containing the template group.

## Template Remote Objects

When a template remote server is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
Remote '<remote_name>' '<operation>' '<container>'
```

- **<remote\_name>** is the name of the remote server.
- **<operation>** can be one of the following:
  - **Created in.** The location where the remote entity was created.
  - **Deleted from.** The location from where the remote entity was deleted.
  - **Updated in.** The location where the remote entity was updated.
- **<container>** is the name of the container containing the remote entity.

## Template Alerts

When a template for an alert is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template Alert  
'<alert_name>' '<operation>' '<container>'
```

- **<alert\_name>** is the name of the object for which the template alert is defined.
- **<operation>** can be one of the following:
  - **Created in.** The location where the template alert was created.
  - **Deleted from.** The location from where the template alert was deleted.
  - **Updated in.** The location where the template alert was updated.
- **<container>** is the name of the template container.

## Template Monitors

When a template for a monitor is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template  
'<monitor_name>' '<operation>' '<container>'
```

- **<monitor\_name>** is the name of the monitor.
- **<operation>** can be one of the following:
  - **Created in.** The location where the template for the monitor was created.
  - **Deleted from.** The location from where the template for the monitor was deleted.
  - **Updated in.** The location where the template for the monitor was updated.
- **<container>** is the name of the container containing the template.

## Alerts

Operations performed on alerts are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Alert
'<alert_name>' '<operation>' '<container>'
```

- **<alert\_name>** is the name of the alert.
- **<operation>** can be one of the following:
  - **Created In.** The location where the new alert was created.
  - **Updated in.** The location where the new alert was updated.
  - **Deleted From.** The location from where the new alert was deleted.
  - **Pasted On.** The user copied information from one alert to another.
- **<container >** is the container of the alert.

## Reports

Operations performed on report definitions are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Report
'<report_name>' '<operation>' '<container>'
```

- **<report\_name>** is the name of the report.
- **<operation>** can be one of the following:
  - **Created In.** The location where a new report was created.
  - **Updated in.** The location where a new report was updated.
  - **Deleted From.** The location from where a new report was deleted.
  - **Pasted On.** The information was copied from one report to another.
- **<container >**. The container of the report.

## Global Search and Replace Operations

Global Search and Replace operations are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: GSAR operation
started
-----
YYYY-MM-DD HH:MM:SS -Global Replace updated group '<group_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated report '<report_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated monitor '<monitor_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated alert '<alert_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated preference '<preference_name>'
-----
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: GSAR operation
finished
```

Start and end operations always appear in the log. The entries appear depending on the actions performed by the Global Search and Replace.

## Login-Logout

Login and logout are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: <message>
```

where **<message>** is either:

- ▶ Logged in.
- ▶ Logged out.

## Failed Login

Failed login attempts are in the format:

```
YYYY-MM-DD HH:MM:SS - Username and password do not match. Failed to login.
```

## Changed Password

Password operations are logged and appear in the following format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: <message>
```

where **<message>** is either:

- Changed password successfully.
- Failed to change password.

## Categories

Operations performed on categories are logged and appear in the following format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Category  
'<category_name>' '<operation>'
```

- **<category\_name>** is the name of the category.
- **<operation>** can be one of the following:
  - **Created.** The location where a new category was created.
  - **Updated.** The location where a new category was updated.
  - **Deleted.** The location from where a new category was deleted.

## SiteScope Server Statistics User Interface

### This section includes:

- General Page on page 1944
- Running Monitors Page on page 1945
- Perfex Process Pool Page on page 1947
- SSH Connections Page on page 1950
- Telnet Connections Page on page 1952

► Log Files Page on page 1954

## General Page

<b>Description</b>	Enables you to view an overview of several key SiteScope server performance statistics, including the current and maximum number of running monitors, waiting monitors, and monitor runs per minute. It also displays a list of monitor types that are currently running, and the number of running instances for each type. <b>To access:</b> Select <b>Server Statistics</b> context > <b>General</b>
<b>Important Information</b>	Only an administrator in SiteScope, or a user granted <b>View server statistics</b> permissions, can view the monitor performance data pages.
<b>Included in Tasks</b>	“Analyze SiteScope Server Statistics” on page 1930
<b>Useful Links</b>	“Using Server Statistics” on page 1922

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Overall Statistics</b>	
<b>Monitors running</b>	The <b>Current</b> column displays the number of monitors queued for execution, based on their update frequency or schedule, that currently have execution threads. This means they are being run.  The <b>Maximum</b> and <b>Measured on</b> columns display the maximum number of monitors that ran and when they ran.



GUI Element	Description
<b>Monitors waiting</b>	<p>The <b>Current</b> column displays the number of monitors queued for execution, based on their update frequency or schedule, that currently are awaiting execution threads. This means they are not being run.</p> <p>The <b>Maximum</b> and <b>Measured on</b> columns display the maximum number of monitors that were waiting at any one time and when this occurred.</p>
<b>Monitors run per minute</b>	<p>The <b>Current</b> column displays a rolling average of the last 10 minutes of monitoring, and tracks the rate (per minute) at which monitors are being run.</p> <p>The <b>Maximum</b> and <b>Measured on</b> columns display the maximum number of monitors running per minute at any one time and when they ran.</p>
<b>Running Monitors by Type</b>	
<running monitors list>	Displays a list of monitor types that are currently running and the number of running instances for each type.

## Running Monitors Page

<b>Description</b>	<p>Enables you to view a list of which SiteScope monitors are running, and which monitors have run recently, at what time, and what was the returned status.</p> <p><b>To access:</b> Select <b>Server Statistics</b> context &gt; <b>Running Monitors</b></p>
<b>Important Information</b>	Only an administrator, or a user granted <b>View server statistics</b> permissions, can view the monitor performance data pages.
<b>Included in Tasks</b>	“Analyze SiteScope Server Statistics” on page 1930
<b>Useful Links</b>	“Using Server Statistics” on page 1922

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Running Monitors</b>	
<b>Run Time</b>	The run time, in seconds, for the monitor that is currently being run.
<b>Skips</b>	The number of skips for the monitor that is currently being run. A SiteScope monitor is reported as skipped if it fails to complete its actions before it is scheduled to run again.
<b>Group Name</b>	The group to which the monitor that is currently being run belong.
<b>Monitor Name</b>	The name of the SiteScope monitor that is currently being run. Clicking the monitor name link opens the Dashboard page for the selected monitor. Monitors with longer run time or skips are colored in red.
<b>Current Status</b>	The status returned by the monitor that is currently being run. For example,
<b>Recent Monitor Runs</b>	
<b>Time and Date</b>	The date and time the monitor ran. The monitors are displayed in the order that have most recently completed running.
<b>Group Name</b>	The group to which the monitor belongs.
<b>Monitor Name</b>	The name of the monitor that SiteScope ran.
<b>Current Status</b>	The status returned by the monitor ( <b>good, warning, error</b> ) and measurement summary details.

## Perfex Process Pool Page

<b>Description</b>	<p>Displays the process manager summary, and pool statistics and statuses for each perfex pool. Perfex is a command line interface to processor event counters. Perfex prints the values of various hardware performance counters after the given command is complete. Perfex_dispatcher is a process used for Microsoft Windows Resources monitors.</p> <p><b>To access:</b> Select <b>Server Statistics</b> context &gt; <b>Perfex Process Pool</b></p>
<b>Important Information</b>	Only an administrator, or a user granted <b>View server statistics</b> permissions, can view the monitor performance data pages.
<b>Included in Tasks</b>	“Analyze SiteScope Server Statistics” on page 1930
<b>Useful Links</b>	“Using Server Statistics” on page 1922

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Process Manager Summary</b>	
<b>Calls per minute</b>	The number of process calls on the SiteScope server, per minute.
<b>Double failures</b>	The number of times SiteScope failed to connect to a remote server, after making two consecutive connection attempts. For connection failure details, check the run monitor and error logs.
<b>Stopped processes</b>	The number of processes that stopped due to error, for example, if the process timed out, since the last SiteScope restart.

GUI Element	Description
<b>Created processes</b>	The number of processes created by SiteScope for all pools since the last restart. If there is a large number of created processes and stopped processes, you should increase the perfex timeout value in <b>Preferences &gt; Infrastructure Preferences &gt; General Settings &gt; Perfex timeout (seconds)</b> .
<b>Cleaned processes</b>	SiteScope cleans processes if they exceed the maximum idle time. The default time before cleaning idle processes is 10 minutes. You can change the idle processes maximum time in <b>Preferences &gt; Infrastructure Preferences &gt; General Settings &gt; Perfex process maximum idle time (minutes)</b> . Cleaning processes improves the memory footprint on the SiteScope machine. Cleaning processes is especially important during a network slowdown when perfexes take longer to finish. As a result, more perfexes are created, but they are not used.
<b>Pool Statistics - perfex/perfex_dispatcher</b>	
<b>Process pool queue length</b>	The number of monitors currently waiting for an available perfex. This value can indicate that there are too many monitors running on perfex, or that the perfex pool is too small.
<b>Average wait time for free process (milliseconds)</b>	The average amount of time to wait, in milliseconds, for a process to be available. If this value exceeds 30,000 milliseconds (30 seconds), monitors will start to fail. A high average wait time indicates that you need to increase the number of processes in the pool.
<b>Average run time (milliseconds)</b>	The average amount of time, in milliseconds, that a perfex takes to run. This gives an indication of the following: <ul style="list-style-type: none"> <li>▶ Network speed. The amount of time it takes to send a request and receive a response from the server.</li> <li>▶ Perfex availability. How long it takes on average to complete the run and to return the perfex to the pool.</li> <li>▶ The number of monitors using perfex.</li> </ul>
<b>Idle processes</b>	The number of processes currently in idle state.

GUI Element	Description
<b>Used processes</b>	The number of processes currently in used state.
<b>Total processes</b>	The total number of processes (idle processes + used processes).
<b>Maximum process pool size</b>	The maximum number of processes allowed per process pool. The default value is 200. You can change the maximum process pool size in <b>Infrastructure Preferences &gt; General Settings &gt; Maximum processes per pool</b> .

 **SSH Connections Page**

<b>Description</b>	Displays Secure Shell (SSH) statistics and a summary of SSH connections when using SSH to connect to remote UNIX or Windows servers.  <b>To access:</b> Select <b>Server Statistics</b> context > <b>SSH Connections</b>
<b>Important Information</b>	Only an administrator, or a user granted <b>View server statistics</b> permissions, can view the monitor performance data pages.
<b>Included in Tasks</b>	“Analyze SiteScope Server Statistics” on page 1930
<b>Useful Links</b>	“Using Server Statistics” on page 1922

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>SSH Statistics</b>	
<b>Total opened</b>	The number of SSH connections opened since the last SiteScope restart.
<b>Total closed</b>	The number of SSH connections closed since the last SiteScope restart.
<b>Total failed to open V1</b>	The number of SSH connections that failed to open using SSH version 1. By default, SiteScope tries to connect using V1 before trying to connect with V2.

GUI Element	Description
<b>Total failed to open V2</b>	The number of SSH connections that failed to open using SSH version 2.
<b>Reused</b>	The number of reused SSH connections since the last SiteScope restart.
<b>Currently allocated resources</b>	The number of SSH connections that are currently open.
<b>Currently in use</b>	The number of SSH connections that are currently open and in use running monitors.
<b>SSH Connections Summary</b>	
<Host name>	<p>For each target remote server, there is a row that displays the following information:</p> <ul style="list-style-type: none"> <li>▶ <b>Machine Name.</b> The name of the monitored remote server.</li> <li>▶ <b>Sessions in Use.</b> The number of open SSH sessions on the monitored remote server.</li> <li>▶ <b>Idle Sessions.</b> The number of idle SSH sessions on the monitored remote server.</li> <li>▶ <b>Maximum Sessions.</b> The maximum number of SSH sessions (idle or in use) on the monitored remote server.</li> <li>▶ <b>Queue Length.</b> The number of SSH sessions in the queue.</li> <li>▶ <b>Average Wait Time.</b> The average amount of time to wait, in milliseconds, for a free SSH session.</li> </ul> <p><b>Note:</b> SiteScope has a limit of 500 concurrent SSH connections.</p>

## Telnet Connections Page

<b>Description</b>	Displays telnet statistics when using telnet to connect to remote UNIX or Windows servers. <b>To access:</b> Select <b>Server Statistics</b> context > <b>Telnet Connections</b>
<b>Important Information</b>	Only an administrator, or a user granted <b>View server statistics</b> permissions, can view the monitor performance data pages.
<b>Included in Tasks</b>	“Analyze SiteScope Server Statistics” on page 1930
<b>Useful Links</b>	“Using Server Statistics” on page 1922

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

Parameter	Description
<b>Telnet Statistics</b>	
<b>Total opened</b>	The number of telnet connections opened since the last SiteScope restart.
<b>Total closed</b>	The number of telnet connections closed since the last SiteScope restart.
<b>Reused</b>	The number of reused telnet connections since the last SiteScope restart.
<b>Currently allocated resources</b>	The number of telnet connections that are currently open.




Parameter	Description
<b>Currently in use</b>	The number of telnet connections that are currently open and in use running monitors.
<b>Telnet Connections Summary</b>	
<Host name>	<p>For each target remote server, there is a row that displays the following information:</p> <ul style="list-style-type: none"> <li>▶ <b>Machine Name.</b> The name of the monitored remote server.</li> <li>▶ <b>Sessions in Use.</b> The number of open telnet sessions on the monitored remote server.</li> <li>▶ <b>Idle Sessions.</b> The number of idle telnet sessions on the monitored remote server.</li> <li>▶ <b>Maximum Sessions.</b> The maximum number of telnet sessions (idle or in use) on the monitored remote server.</li> <li>▶ <b>Queue Length.</b> The number of telnet sessions in the queue.</li> <li>▶ <b>Average Wait Time.</b> The average amount of time to wait, in milliseconds, for a free telnet session.</li> </ul> <p><b>Note:</b> SiteScope has a limit of 500 concurrent telnet connections.</p>

## Log Files Page

<b>Description</b>	Enables you to inspect the SiteScope log files. <b>To access:</b> Select <b>Server Statistics</b> context > <b>Log Files</b> .
<b>Included in Tasks</b>	<ul style="list-style-type: none"> <li>➤ “Analyze SiteScope Server Statistics” on page 1930</li> <li>➤ “Configure the Audit Log” on page 1931</li> </ul>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Using Log Files” on page 1927</li> <li>➤ “SiteScope Log File Columns” on page 1932</li> <li>➤ “Audit Log Entries” on page 1933</li> <li>➤ “Audit Log Limitations” on page 1929</li> </ul>

### Log Files Table

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Change the sort order in the columns by clicking the arrow in the column title. A small up or down arrow is displayed to the left of the arrow which indicates the sort order.  <b>Note:</b> Clicking the arrow in the <b>Type</b> column title opens the list of log types, which enables you to filter the list by the log type you want to display. To clear the filter, click the arrow again, and select <b>(All)</b> .
<b>Type</b>	The log file type. For details on the different types of log files, see “Log File Types” on page 1955.
<b>Log File</b>	The name of the log file. Double-click a log file link to open the file in your Web browser.
<b>Size</b>	The size of the log file.
<b>Last Modified</b>	The time and date on which the log file was last modified.

## Log File Types

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Audit Logs</b>	Contains links to the logs containing all configuration changes that were performed, such as creation of monitors, templates, alerts and so on. For details on audit logs, see “Using the Audit Log” on page 1928.
<b>BAC Integration Logs</b>	Contains information about connectivity and monitor data transfer when SiteScope is configured to report to HP Business Availability Center.
<b>Daily Logs</b>	Contains links to the logs containing individual monitor measurements. SiteScope creates a new monitor log each day to record all monitors run during that 24 hour period. These logs are the basis for SiteScope Reports. <b>Note:</b> The monitor logs can become very large depending on the monitor environment. This may make it impractical to view them using a Web browser.
<b>Error Logs</b>	Contains a variety of messages relating to the operation of SiteScope. This includes a record of errors that SiteScope may have encountered when trying to perform monitor actions or data communication actions. It also includes messages indicating when SiteScope was stopped or started and if there are monitors that are skipping because they are unable to complete their task.
<b>Run Monitor Logs</b>	Records information when specific monitor runs and some actions related to managing monitors. This can be useful in troubleshooting monitors.

GUI Element	Description
Other Logs	<p>Contains various different log file types, such as:</p> <ul style="list-style-type: none"> <li>▶ <b>alert.log.</b> Records alert information whenever SiteScope generates an alert. This can be used to troubleshoot alert actions and to confirm that alerts were sent.</li> <li>▶ <b>monitorCount.log.</b> Counts the total number of monitors and license points used in SiteScope. It also specifies the number and license point usage for each type of server health monitor. This log is updated once a day when SiteScope starts (and not on every change). You can refresh the log file at any time by selecting <b>Help &gt; About SiteScope</b>.</li> <li>▶ <b>Operator Log.</b> An optional log file used to record SiteScope operator actions, primarily information from use of the Acknowledgement function. This log is created when an acknowledgement is added to one or more monitors.</li> <li>▶ <b>Post Log File.</b> An optional log file used to record HTTP Post requests made to the SiteScope server. This can be used to track administrative actions performed. This log is only enabled when the <code>_postLogFile=true</code> setting exists in the <b>master.config</b> file.</li> <li>▶ <b>silent_deployment.</b> Records details on submitted requests for silent deployments and their corresponding deployment results. It also includes error messages for silent deployments that fail. This log is updated once a day when SiteScope starts (and not on every change).</li> <li>▶ <b>URL Details.</b> An optional log file used to record the complete contents of HTTP and HTTPS requests made by SiteScope URL monitor types. This can be used to troubleshoot URL and URL Sequence monitor types. This log is only enabled when the <code>_urlDetailLogEnabled=true</code> setting exists in the <b>master.config</b> file. This can be used selectively by adding the <code>_urlDetailLogEnabled=true</code> setting into an individual monitor group configuration file that contains a URL monitor type.</li> </ul>

# Part IX

---

## Alerts and Reports



## SiteScope Alerts

This chapter includes the main concepts, tasks, and reference information for SiteScope Alerts.

### **This chapter includes:**

#### **Concepts**

- SiteScope Alerts Overview on page 1960
- Creating Alert Actions on page 1963
- Understanding When SiteScope Alerts Are Sent on page 1964
- Customizing Alert Templates on page 1969
- Working with Database Alerts on page 1971
- Working with Disable or Enable Monitor Alerts on page 1972
- Working with Email Alerts on page 1973
- Working with Log Event Alerts on page 1974
- Working with Pager Alerts on page 1975
- Working with Post Alerts on page 1976
- Working with Script Alerts on page 1977
- Working with SMS Alerts on page 1981
- Working with SNMP Trap Alerts on page 1982
- Working with Sound Alerts on page 1983

#### **Tasks**

- Configure an Alert on page 1984
- Customize an Alert's Message Content on page 1986

- ▶ [Customize Alert Template Tag Styles on page 1988](#)

#### Reference

- ▶ [SiteScope Alert Templates Directory on page 1989](#)
- ▶ [SiteScope Alert Template Properties Directory on page 1990](#)
- ▶ [SiteScope Alerts User Interface on page 1997](#)

## SiteScope Alerts Overview

SiteScope alerts are notification actions that are triggered when the conditions for the alert definition are detected. You use an alert to send some notification of an event or change of status in some element or system in your infrastructure. For example, an alert can be triggered when a SiteScope monitor detects a change from Good to Error indicating that the monitored system has stopped responding.

An alert definition contains settings that tell SiteScope what monitors can trigger the alert, what condition to watch for, what information to send, and who should be the recipients of the alert. For example, you can create an alert that includes instructions for SiteScope to send the specific server address and error code to your pager or email when an error condition is detected on a particular system. You can also have SiteScope respond to problems by automatically initiating recovery or action scripts with Script Alert. For example, you can configure a Script Alert to run a script to restart a server if a monitor detects that a system is no longer responding and CPU utilization has reached 100%. For details on the alert types, see “Action Type Dialog Box” on page 2006.

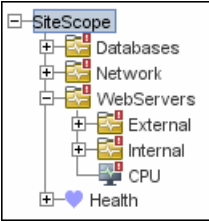
SiteScope alerts can be configured in several ways. Alerts can be associated with one or more individual monitors, with one or more groups of monitors, a combination of monitors and groups, or globally for all monitors and groups. Global and group-wide alerting is generally the most efficient but may not provide the needed control.

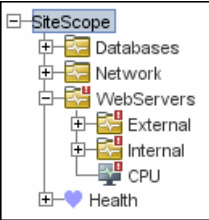
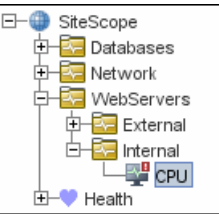


You can use the **Filter Settings** function on each alert definition page to create filter criteria to control global and group alerts to more specific criteria. Filter criteria can be used to restrict the alert to only monitors of a certain type, that contain a certain text string, or other filter criteria. For example, creating a global alert with a filter criteria for CPU Monitor creates an alert that is triggered only for the CPU monitor type. For details on how to configure alerts, see “SiteScope Alerts Page” on page 1997.

## Alert Associations and Considerations

The table below displays an overview of the different alert associations and considerations.

Alert Class	Description
Global Alerts	<p>Alerts that are triggered when any monitor on a given SiteScope reports the category status defined for the alert.</p> <p>New groups and monitors added after the alert definition is created are automatically associated with the alert.</p> <p>The following display is an example of a global alert associated with the SiteScope node. All monitors can trigger this alert.</p>  <p><b>Note:</b> We do not recommend creating a global alert because the alert can potentially be triggered by every group and monitor within SiteScope.</p>

Alert Class	Description
<p>Group Alerts</p>	<p>Alerts that are triggered when any monitor within the associated group or groups reports the category status defined for the alert.</p> <p>The following is an example of a group alert. Any monitor or subgroup within the group WebServers can trigger this alert.</p>  <p>New subgroups and monitors added within the associated group or groups after the alert definition is created are automatically associated with the alert.</p>
<p>Individual Monitor Alerts</p>	<p>Alerts that are triggered when an associated monitor reports the category status defined for the alert.</p> <p>The following is an example of an individual monitor alert. Only the associated monitor can trigger this alert.</p>  <p>New monitors added after the alert definition is created are not automatically associated with the alert but can be added by editing the alert definition.</p>

You can create as many SiteScope alert definitions as required. However, you should plan and consolidate alerts to keep the number of alert definitions to a minimum. This facilitates alert administration and helps reduce redundant alert messages or actions.

## Creating Alert Actions

When you create an alert scheme in SiteScope, you create alert actions to be triggered when the alert conditions are met. You create alert actions using the Alert Action dialog box. While in the dialog box, you determine the following:

- ▶ The type of alert action. For a detailed list of available alert actions, see “Action Type Dialog Box” on page 2006.
- ▶ The settings for the type of alert being sent. For example, you can define the recipients and their addresses for an email alert action.
- ▶ The status condition that triggers the alert. For example, you can instruct SiteScope to trigger an alert action when a monitor’s status changes to error or unavailable.
- ▶ The trigger settings that determine when the alert is triggered and when it is sent. For details, see “Understanding When SiteScope Alerts Are Sent” on page 1964.

You can create multiple alert actions for an alert scheme.

- ▶ **Multiple methods of delivery.** You can create an alert action to send a sound alert and another alert action to send an email alert. Both are sent when the alert is triggered.
- ▶ **Schedule-dependent delivery.** You can also set different schedules for the different actions within the same alert definition. For example, you can schedule an email alert action to be sent during regular working hours and an SMS alert action for evening and night hours. Both are triggered by the same change in condition but are sent at different times, depending on when the alert is triggered.
- ▶ **Action dependencies.** You can also make one alert action dependent on another alert action. This enables you to instruct SiteScope to send one type of alert when the trigger condition is first met and send another type of alert only when the first type of alert has been sent a number of times.

You can copy an alert action into other monitors or groups for use by other alerts. To use alert actions for other alerts, you must copy the alert and paste it into another monitor or group. All the alert actions for the alert are copied into the new alert. You can then edit the alert to be triggered for the new target monitor or group.

For details on working with different alert types, see “Action Type Dialog Box” on page 2006.

## Understanding When SiteScope Alerts Are Sent

SiteScope triggers the alert as soon as any monitor it is associated with matches the alert trigger condition. The trigger settings options in the Alert Action dialog box enable you to control when alerts are actually sent in relation to when a given condition is detected. For example, you can choose to have SiteScope send an alert only after an error condition persists for a specific interval corresponding to a given number of monitor runs. This is useful for monitors that run frequently that monitor dynamic, frequently changing environment parameters. In some cases, a single error condition may not warrant any intervention. For details about configuring trigger settings, see “Trigger Frequency Panel” on page 2025.

The following examples illustrate how different alert configurations send alerts after the error condition has persisted for more than one monitor run. It is important to note that the sample interval corresponds to how often the monitor is run. If a monitor runs every fifteen seconds and the alert is set to be sent after the third error reading, the alert is sent 30 seconds after the error was detected. If the monitor run interval is once every hour with the same alert setup, the alert is not sent until 2 hours later.

**Example 1 - Always, after the condition has occurred at least N times**

**Example 1a.** An alert is sent for each time monitor is in error after condition persists for at least three monitor runs. Compare this with Example 1b below.

Alert setup	Always, after the condition has occurred at least 3 times								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=3 alert!	c=4 alert!	c=5 alert!	c=0	c=1	c=2

**Example 1b.** An alert is sent for each time monitor is in error after condition persists for at least three monitor runs. Shows how the count is reset when the monitor returns one non-error reading between consecutive error readings. Compare this with Example 1a above.

Alert setup	Always, after the condition has occurred at least 3 times								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=0	c=1	c=2	c=3 alert!	c=0	c=0

**Example 2 - Once, after the condition has occurred exactly N times**

An alert is sent only once if monitor is in error for at least three monitor runs, regardless of how long the error is returned thereafter.










<b>Alert setup</b>	Once, after the condition has occurred exactly 3 times								
<b>sample interval</b>	0	1	2	3	4	5	6	7	8
<b>status</b>									
<b>count</b>	c=0	c=1	c=2	c=3 alert!	c=4	c=5	c=6	c=7	c=8

**Example 3 - Initially, after X times, and repeat every Y times**

**Example 3a.** An alert is sent on the fifth time monitor is in error and for every third consecutive error reading thereafter. Compare this with Example 3b below.

<b>Alert setup</b>	Initially, after 5 times, and repeat every 3 times								
<b>sample interval</b>	0	1	2	3	4	5	6	7	8
<b>status</b>									
<b>count</b>	c=0	c=1	c=2	c=3	c=4	c=5 alert!	c=6	c=7	c=8 alert!

**Example 3b.** An alert is sent on the third time monitor is in error and for every fifth consecutive error reading thereafter. Compare this with Example 3a above.

Alert setup	Initially, after 3 times, and repeat every 5 times								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=3 alert!	c=4	c=5	c=6	c=7	c=8 alert!

#### Example 4 - Configuring Multiple Alerts

Because you can create multiple alerts and associate more than one alert to a monitor, you can tell SiteScope to take more than one action for a given situation. For example, you can create one alert that tells SiteScope to page you whenever any monitor returns an error status. You can then create another alert that tells SiteScope to run a script file to delete files in the /tmp directory on your server if your Disk Space Monitor returns an error. If your disk becomes too full, SiteScope would page you because of the first alert definition and would run the script to delete files in the /tmp directory because of the second alert definition.

SiteScope alerts are generated when there is a change in state for a monitor reading. Thus you can set an alert for OK or warning conditions as well as error conditions. One way to take advantage of this is to add two alerts, one alert on error, and one alert on OK. Set alerts to be sent after the condition is detected 3 time. For the OK alert, check the box marked **Only alert if monitor was previously in error at least 3 times**. This prevents unmatched OK alerts, such as when a monitor was disabled for any reason (manually, by schedule, or by **depends on**) and then starts up again. This can also be used so that an OK alert is only sent after a corresponding error alert was sent. With these two alerts, you get a page when a link or service goes down (monitor detects change from OK to error), and another when it comes back up (monitor detecting change from error to OK).

The following is an example of using two alerts with a monitor. An Alert on error sent once for error after condition persists for at least three monitor runs. Alert on OK sent once for good status after at least one error or warning interval.

<b>Alert on Error Setup</b>	<b>On Error</b>		<b>Once, after the condition has occurred exactly 3 times</b>						
<b>Alert on OK Setup</b>	<b>On OK</b>		<b>Once, after the condition has occurred exactly 1 times and Only alert if monitor was previously in error at least 3 times</b>						
<b>Sample Interval</b>	0	1	2	3	4	5	6	7	8
<b>Status</b>									
<b>Count</b>	c=0	c=1	c=2	c=3 alert!	c=4	c=5	c=6	c=7	c=1 alert!

Once the monitor's status changes, the relevant status count is reset to zero.



## Customizing Alert Templates

SiteScope uses templates when generating alert messages and reports. In most cases, you select the template you want to use in the Alert page when you create an alert. You can customize the existing templates or create your own by making a copy of an existing template. You customize the alert templates by adding or removing text, by adding property variables, or changing the order of text or property variables that are included in the template.

---

**Note:** We recommend that you create custom alert templates using new filenames. If you modify one of the default templates provided with SiteScope and save the changes to the same file, the changes that you make may be lost if you reinstall SiteScope or upgrade the SiteScope installation.

---

To make a custom alert template available to SiteScope, you must save any customized alert templates into the directory containing the templates for the applicable alert type. For the list of directory names containing SiteScope alert templates you can copy and customize, see “SiteScope Alert Templates Directory” on page 1989.

The templates in these groups are text files that include property variable markers. You use a text editor to create or modify these templates. The new templates saved into the directories shown become available to the applicable alert on the Alert page.

For details on customizing alert template settings, see “Customize an Alert’s Message Content” on page 1986 and “Customize Alert Template Tag Styles” on page 1988.

### Example - Typical Template Used for the Email Alert

The following is an example of the default template used for the Email Alert. The first section is the alert header. The first line in the alert header includes a link to the SiteScope installation which sent the problem. This provides you with a way to access the SiteScope installation reporting the problem.

Below the link is a block of text that further summarizes what caused the alert. This includes:

- ▶ the name of the monitor that triggered the alert
- ▶ the group to which the monitor belongs
- ▶ the alert status reported by the monitor
- ▶ the sample ID number indicating how many times the monitor ran before the condition was reported
- ▶ the time of day when the error occurred

```
This alert is from SiteScope at <SiteScopeURL>
Monitor: <groupID>:<name>
Group: <group>
Status: <state>
Sample #: <sample>
Time: <time>
-----Detail -----
<mainParameters>
<mainStateProperties>
```

The names that appear within <brackets> are property variable markers. When the alert is generated, SiteScope replaces these markers with the corresponding values of the variable for the monitor or monitor group that has triggered the alert.

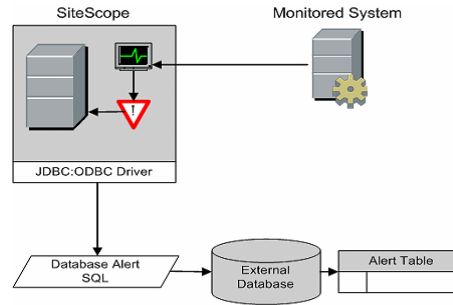
You add or edit the text portions of the template. For example, you could change the first line of the template above to read:

```
A Web monitoring alert was generated by the SiteScope installation found at
<SiteScopeURL>
```

## Working with Database Alerts

Database alerts can forward system fault data and other status information to any SQL-compliant database.

The following diagram illustrates the Database alert.



You need the following to be able to use the Database alert type:

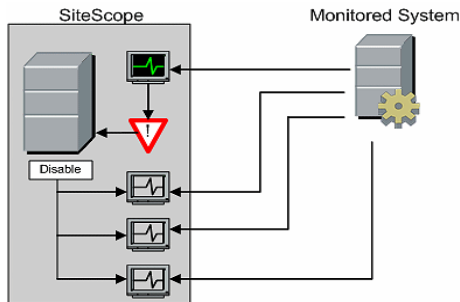
- Access to a SQL compliant database.
- The applicable database connection URL which the SiteScope server uses to connect to the database.
- Installation of the applicable database middleware driver that the SiteScope application uses to communicate with the database on the SiteScope server.
- Database tables that have been created and structured to match the corresponding SQL statement that SiteScope uses to enter the alert into the database.

For details on how to configure an alert, see “Configure an Alert” on page 1984.

## Working with Disable or Enable Monitor Alerts

Disable or Enable Monitor alerts can turn off and turn on the triggering of alerts for monitors. This is useful for times when server maintenance or other activities are being performed that would logically result in errors for some monitors and cause unnecessary alerts to be generated.

The following diagram illustrates an example of this alert type used to disable several monitors based on the condition reported to one monitor.

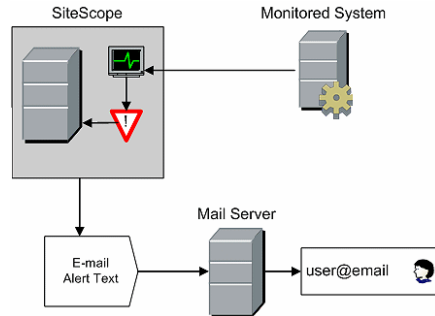


This alert type provides a functionality similar to the **Depends on** function for building group dependencies between monitors and monitor groups. One important difference is that monitors disabled by this type of alert are not automatically re-enabled when the status of the subject monitor or group changes back to the original state. You can create one alert with an **Alert Category** of **Error** that disables monitors. You can then create a second alert with an **Alert Category** of **Good** that enables the same monitors.

For details on how to configure an alert, see “Configure an Alert” on page 1984.

## Working with Email Alerts

Email alerts send event notifications from SiteScope to a designated email address as seen in the following diagram.



You need the following to be able to use the Email alert type:

- Access to an active email server
- One or more email accounts that can receive the email alerts
- SiteScope Email Preferences set to work with the external email server

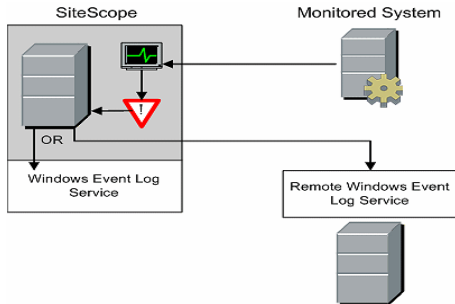
For more information on configuring SiteScope email recipients, see “Email Preferences” on page 1461.

For details on how to configure an alert, see “Configure an Alert” on page 1984.

## Working with Log Event Alerts

Log Event alerts can be used to extend the types of events that are logged to a Windows Application Event Log. This provides a way to forward event data to log query systems that may not normally be logged by the Windows operating system.

The following diagram illustrates the Log Event alert.



You need the following to be able to use the Log Event alert type:

- ▶ Access to the Windows Event Log service. By default, this is the Event Log on the machine where SiteScope is running. The alert definition can be configured to send log events to another server.
- ▶ SiteScope running on a Microsoft Windows platform.

---

**Important:** If you are using SiteScope's Microsoft Windows Event Log Monitor, you must use care when using the Log Event alert type because it is possible to create an endless loop condition that can fill your Event log file. This can happen when a Microsoft Windows Event Log Monitor detects an event that triggers a Log Event alert, which in turn puts a new event into the event log, which the Event Log Monitor then detects, and then triggers the Log Event alert, and so forth. To avoid this, Log Event alert types should not be associated with Microsoft Windows Event Log Monitors.

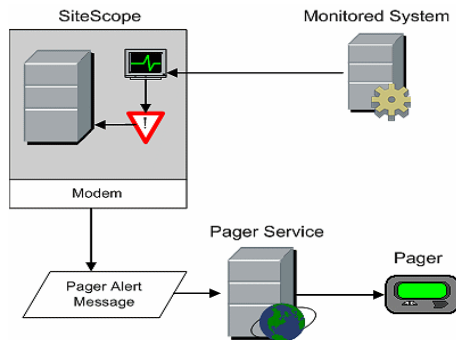
---

For details on how to configure an alert, see “Configure an Alert” on page 1984.

## Working with Pager Alerts

Pager alerts can be used to send event notification to electronic pagers. This is particularly useful when access to email may not be available. Depending on the type of pager you use and the capabilities of the pager service, you can configure the Pager Alert to send a pager message with an abbreviated description of the problem or detected condition.

The following diagram illustrates the Pager alert.



You need the following to be able to use the Pager alert type:

- ▶ Access to an active pager service
- ▶ A modem which the SiteScope server can use to connect to the pager service
- ▶ One or more pagers that can receive the pager alerts
- ▶ SiteScope Pager Preferences set to work with the modem and pager service

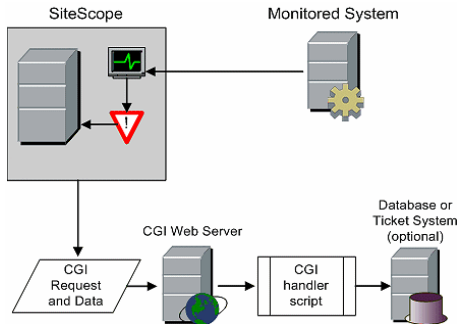
For more information on configuring SiteScope to use pager alerts, see “Pager Preferences” on page 1471.

For details on how to configure an alert, see “Configure an Alert” on page 1984.

## Working with Post Alerts

Post alert use the Common Gateway Interface protocol to forward POST data to a CGI enabled program. This can be used to forward event data to CGI script on another server that is a front-end for a trouble ticket system or reporting database. This alert type also provides a way of sending alert information through a firewall using HTTP or HTTPS without having to make other security changes.

The following diagram illustrates the Post alert.



You need the following to be able to use the Post alert type:

- ▶ HTTP access between the SiteScope server and the server running the CGI script or server.
- ▶ Format and syntax of the CGI POST request to the applicable CGI script or server.

For details on how to configure an alert, see “Configure an Alert” on page 1984.



## Working with Script Alerts

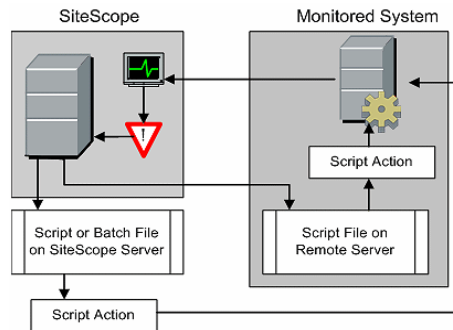
Script alerts can automatically initiate recovery scripts. You can configure a Script alert to run a command to restart a server or a service.

The most important components of Script Alerts are:

- The script definition itself.
- The monitor or monitors that are assigned to trigger the alert.
- The script to be run by the alert.

The alert message template and resulting alert message file may also need to be considered depending what the script needs to do. You can use a script template, together with the **Parameters** setting to pass data to your script.

The following diagram illustrates the general concept of the script alert for both a local script and a script on a remote host.



The script alert definition or instance and the monitor or monitors that trigger the alert are handled as with other alerts or monitors in SiteScope. For example, you may create a monitor to watch a Web server running on a remote UNIX server. You can create a Script Alert associated with that monitor that runs a script to kill and restart the Web server process if the monitor reports an error.

This section includes the following topics:

- “Managing Script Files” on page 1978
- “Passing Data to a Script” on page 1979
- “Running Different Types of Scripts” on page 1980
- “Troubleshooting Scripts” on page 1980

## Managing Script Files

Creating the script file to be called or run by the Script Alert definition is another key step in using this automation capability in SiteScope. The specific commands and actions taken by the script are up to you. The script file should be written as a plain text file compatible with the operating system where the script is to be run. This may be the same server where SiteScope is running or it may be on a remote machine to which SiteScope has access.

To run a script on the machine where SiteScope is running, the script file must be saved in the **<SiteScope root directory>\scripts** directory on the SiteScope machine where the Script Alert is defined.

To run a script on a remote machine, you must save the script in a directory called **\scripts** in the home directory tree for the user account that SiteScope has execute permissions for on the remote machine.

The current execution directory when a script is run is **<SiteScope root directory>\classes\** and not the **<SiteScope root directory>\scripts\** directory. For commands run by the script itself, the relative execution directory is **<SiteScope root directory>\classes\**. Use full paths for any other file system commands or programs called by your script so that you do not need to worry about the current directory. Also, the server system environment variables may not have been set up for the script execution. This is another reason to use full paths for executables called by the script. If a script works when you run it from the command line but not from SiteScope, then you must determine what the error is.

## Passing Data to a Script

SiteScope passes a number of parameters to the script as command line arguments. You can use this option to pass data to a script that can be used to modify a script's action. This adds versatility to the Script Alert. By default, a SiteScope Script Alert passes seven command line arguments to a script. These are:

- The path of the scripts directory.
- The name of the monitor that caused the alert.
- The current status of the monitor.
- The path to the Alert Message File.
- The ID code of the monitor.
- The group the monitor is in.
- Any additional parameters specified on the **Parameters** text box in the alert form.

Two of these default arguments allows the script to access even more data. One is the Alert Message File and the other is the **Parameters** text box. The Alert Message File is a temporary text file created by SiteScope based on the alert template chosen for the Script Alert instance. Depending on the template you create or use, the Alert Message File may contain custom information as well as data specific to the monitor that triggered the alert. By passing the path to the Alert Message File to the script, you can have the script access this data.

You use the Parameters text box to specify individual monitor parameter data to be passed to the script. You can include multiple parameters by separating the parameters with spaces. This effectively allows you to increase the total number of parameters passed to the script.

The path of the scripts directory can be useful in setting a execution path to another program as well as setting a directory path for any output written by the script.

For more information and examples of passing parameters and data to scripts, see “Writing Scripts for Script Alerts” on page 2029.

## Running Different Types of Scripts

You can run non-batch scripts, for example VBScript or Perl scripts, without wrapping them into a batch file (in versions of SiteScope earlier than 9.50, this was not possible).

- ▶ You can see scripts with any extensions by adding the `_scriptExtensions` property to the **master.config** file. For example, to see **.pl**, **.py**, or **.php** scripts, use the following format:  
`_scriptMonitorExtensions=.pl;.py;.php`
- ▶ You can run script interpreters with script extensions by adding the `_scriptInterpreters` property to the **master.config** file as follows:  
`_scriptInterpreters=pl=c:/perl/perl.exe;py=c:/python/python.exe;php=c:/php/php.exe`

## Troubleshooting Scripts

- ▶ The scripts are run with the permissions of the account used by the SiteScope service. Some scripts may need extra permissions and you must use the Services control panel to change the login account for SiteScope and then stop and start SiteScope. For example, scripts that restart services or reboot remote machines or scripts that copy protected files.
- ▶ Because the script is run by the SiteScope service, anything done as part of your login may not have occurred in the script. For example, you can not rely on mapped drives, environment variables, or other login script items. In addition, it cannot receive any interactive input from a keyboard or other input device. Any script action or command that requires a user confirmation or input would cause the script to hang. Do not include any interactive commands requiring a user action as part of the script. Also, opening a WIN32 application (for example, Notepad) also causes the script to hang because it is waiting for the user to exit or close the application before continuing with the script execution.
- ▶ If there are quotation marks in the Script Alerts status summary, SiteScope doubles the quotation marks in the Script Alert results. You should take this into account when defining a content match filter.

For details on how to configure an alert, see “Configure an Alert” on page 1984.

## Working with SMS Alerts

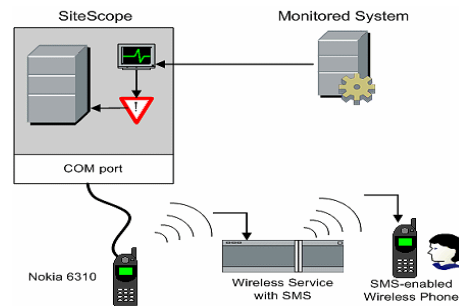
SMS alerts are designed to transmit the name of the SiteScope monitor that has reported an event condition and the status of that monitor as the content of the message. It is an alternative to the Pager alert for communicating event notifications to mobile users without using email.

---

**Note:** At present, the SMS alert can only be sent from SiteScope by using the hardware specified in this section. For alternative ways of sending SMS messages using SiteScope, see the HP Software Self-solve knowledge base (<http://h20230.www2.hp.com/selfsolve/documents>). To enter the knowledge base, you must log in with your HP Passport ID.

---

The following diagram illustrates the SMS Alert.



You need the following to be able to use the SMS alert type:

- ▶ An available serial communications port on the SiteScope machine that is sending the SMS alerts.
- ▶ A serial-to-wireless device interface cable, RS-232 Adapter Cable Nokia DLR-3P to connect the wireless transmitting device to the machine where SiteScope is running.
- ▶ An SMS-enabled wireless device connected to the SiteScope machine that is sending the alerts (that is, the Nokia 6310 phone using the interface cable).
- ▶ The necessary software to enable the SMS Alert (normally included with SiteScope 7.6c1 and later).

---

**Note:** Make sure that you do not have Nokia Data Suite, Palm Hot Sync, or any PDA software running on the server where SiteScope is running. These programs can bind the COM ports and prevent the dialer from working correctly.

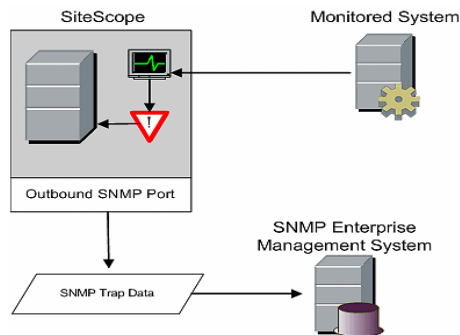
---

For details on how to configure an alert, see “Configure an Alert” on page 1984.

## Working with SNMP Trap Alerts

SNMP Trap alerts forward event data from any type of SiteScope monitor to an SNMP enabled host or management system. This means that SiteScope can be used to monitor and report events for applications and systems that do not have their own SNMP agent. For example, this can be used to send measurement data from a SiteScope Microsoft Windows Performance Counter based monitor type or a URL monitor in the form of an SNMP trap.

The following diagram illustrates the SNMP Trap Alert.



You need the following to be able to use the SNMP trap alert type:

- Access to the applicable SNMP network ports
- SiteScope SNMP Preferences set to work with the applicable SNMP management console

For more information on configuring SiteScope to use SNMP alerts, see “SNMP Trap Preferences” on page 1481.

For details on how to configure an alert, see “Configure an Alert” on page 1984.

## Working with Sound Alerts

Sound alerts play a sound or audio file on the machine on which SiteScope is running when an alert is generated. The alert is effective only if the SiteScope server is in an area regularly occupied by support staff and the server is equipped with a sound card capable of processing the associated sound file.

Alternatively, SiteScope can be configured to embed an alert audio file into the Web pages served by SiteScope. This audio file is included with any SiteScope page that includes an error status for any monitor, such as the main panel or group detail pages. While this allows audio notification to all SiteScope clients through the user interface, it is not a true SiteScope alert and thus does not enable the same configuration options as the Sound Alert. For information about how to configure SiteScope to embed audio files for error notification, refer to the HP Software Self-solve knowledge base ([h20230.www2.hp.com/selfsolve/documents](http://h20230.www2.hp.com/selfsolve/documents)). To enter the knowledge base, you must log in using your HP Passport ID.

For details on how to configure an alert, see “Configure an Alert” on page 1984.

## **Configure an Alert**

This task describes the steps involved in configuring an alert definition.

This task includes the following steps:

- “Create an Alert” on page 1984
- “Test the Alert” on page 1985
- “Customize an Alert’s Message Content” on page 1985
- “Customize Alert Template Tag Styles” on page 1988
- “Results” on page 1985

### **1 Create an Alert**

You can create a new alert or copy an existing alert into any group or monitor container in the SiteScope tree.

- **Create a new Alert.** Right-click the container to which you want to associate the alert, and select **New > Alert**. Enter a name for the alert, select the targets to trigger the alert, and configure an alert action. For details on the user interface, see “New/Edit Alert Dialog Box” on page 1999.
- **Copy an Alert Definition.** In the Alerts tab, select the alert you want to copy, and paste it into the desired group or monitor container. The alert target automatically changes to the group or monitor into which the alert is copied.

---

**Important:** If you copy an alert definition from one group container to another, the **Alert targets** for the pasted alert are automatically reset to include all of the children of the container into which the alert is pasted. After pasting an alert, edit the alert definition properties to be sure that the assigned **Alert targets** are appropriate to the new alert context and your overall alerting plan.

---



## 2 Test the Alert

Select the alert in the Alerts tab of the monitor tree and click **Test**. Select the monitor instance you want to test and click **OK**. A dialog box opens with information about the alert test.

---

**Note:** The monitor you select does not have to be reporting the same status category that is selected to trigger the alert to test the alert. For example, the monitor does not have to currently be reporting an error to test an alert that is triggered by error conditions.

---



## 3 Customize an Alert's Message Content

Customize SiteScope alert templates to alter the content and format of alert messages. For details on how to perform this task, see “Customize an Alert's Message Content” on page 1986.

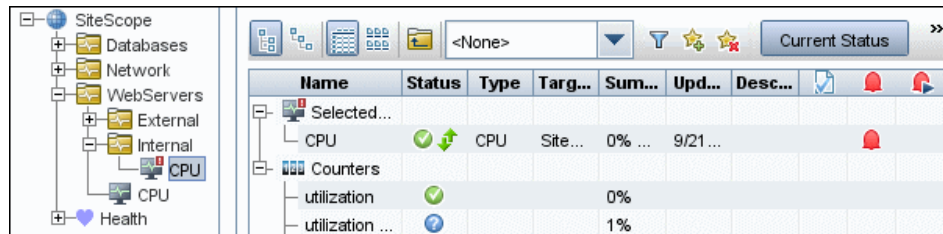
## 4 Customize Alert Template Tag Styles

Customize SiteScope alert templates tag styles if you have a parser that needs a specific delimiter or to change the bracket delimiters used to identify variables. For details on how to perform this task, see “Customize Alert Template Tag Styles” on page 1988.





## 5 Results

An alert is added to the specified container in the monitor tree (indicated by the  icon). The alerts icon  is also displayed in SiteScope Dashboard next to each group or monitor that has one or more configured alerts.

### Example



The screenshot shows the SiteScope interface. On the left is the monitor tree with 'WebServers' expanded to 'Internal' and 'CPU' selected. On the right is the dashboard for the selected CPU monitor. The dashboard includes a table with the following data:

Name	Status	Type	Targ...	Sum...	Upd...	Desc...			
Selected...									
CPU		CPU	Site...	0% ...	9/21 ...				
Counters									
utilization				0%					
utilization ...				1%					

## **Customize an Alert's Message Content**

This task describes how to customize SiteScope alert templates to alter the content and format of alert messages.

**To customize an alert's message content and format:**

- 1** Open a text editor that has access to the alert template directories on the SiteScope machine.  
  
For a list of the directory names containing SiteScope alert templates, see “SiteScope Alert Templates Directory” on page 1989.
- 2** Open an existing template file of the alert type you want to customize within a text editor.
- 3** Make changes to the template. Depending on the alert type, you can add or remove text, change the order of text or property variables, or add other property variables. To add specific properties, add the applicable property variable name between < > bracket pairs to the template.
- 4** Save the changes to a unique filename within the directory for the applicable alert type.

---

**Note:** The new template is added to the Action Type Settings Template drop-down list.

---

**Example - Shortening an Email Alert Message**

You can shorten the length of an email alert by removing properties that provide unneeded information. For example, if there is no added value in reporting the time of a specific alert, you can remove the `<time>` property from the template.

---

**Tip:** It is recommended that you use the Typical template (the default setting) as a base for your customized template.

---

In the `<SiteScope root_directory>\templates.mail` directory, open the **Typical** template file. Remove the line `Time: <time>`. Save the changes to a new filename.

**Example - Changing an SNMP Alert Message**

You can change the SNMP Alert message from displaying the SNMP monitor's status to displaying a list of counters that are in Error state along with their values. This causes the message to only contain counters that breached the Error threshold and to omit all other counters.

In the `<SiteScope root dir>\templates.SNMP` directory, open the **Default** template file in a text editor. The file contains the line:

```
SiteScope\<group>\<name>\<sample>\<state>\
```

Replace the string `<state>` with the string `<errorOnly>`. The angle brackets (`<`,`>`) must remain around the text.

---

**Note:** If you want to display a list of counters that are in Warning state, replace the string `<state>` with the string `<warningOnly>`.

---

Edit `<SiteScope root dir>\groups\master.config` file and add the line `_errorOnlyDelimiter=,`

with other similar error definitions.

In this example, the delimiter is a comma (,), but you can also use a space (" ") or a tab (\t). The added line in **master.config** looks something like:

```
_errorInsertHTML=
_errorOnlyDelimiter=,
_errorOnlyNewlineFormat=true
```

---

**Note:**

- ▶ If you used the string **<warningOnly>**, you must use the string **\_warningOnlyDelimiter=<delimiter>** in **master.config**.
  - ▶ If no **\_errorOnlyDelimiter** is defined in **master.config**, the default delimiter is a space (" ").
- 

## **Customize Alert Template Tag Styles**

This task describes how to change the delimiter between items in the list if, for example, you have a parser that processes alert messages and needs a specific delimiter. You can also change the bracket delimiters that are used to identify variables. This is useful if you want the message read by XML and a variable replaced by an XML string.

**To change the bracket delimiter:**

- 1** Edit the template file for which you want to change the bracket delimiter. For example: `<SiteScope root directory>\templates.mail\`.
- 2** Use a text editor to add the following lines to the top of the relevant file:

```
[Tag-Style:{}]
```

Enter the characters after the colon (in this example {}) that should be used as the delimiter instead of the html brackets (<>).

- 3** Edit the relevant variables to be bracketed by the new characters defined in the Tag-Style string. For example: `{state}`.

## SiteScope Alert Templates Directory

The following is a list of the directory names containing SiteScope alert templates you can copy and customize.

Template Group	Description	Location
Event Log	Format and content of data written into event logs.	<SiteScope root directory>\ templates.eventlog
History	Format and content of email messages that notify recipients that a report has been generated.	<SiteScope root directory>\ templates.history
Email	Format and content of alert messages sent by email.	<SiteScope root directory>\ templates.mail
Template	Group, Description, Location, Pager Format, and content of pager alerts.	<SiteScope root directory>\ templates.page
Post	Format and content of messages submitted to a CGI script by a post alert.	<SiteScope root directory>\ templates.post
Script	Format and content of messages sent to a script when a script alert is triggered.	<SiteScope root directory>\ templates.script
SNMP	Format and content of messages sent by SNMP when a SNMP trap is triggered.	<SiteScope root directory>\ templates.snmp

## SiteScope Alert Template Properties Directory

The following is a list of the common properties found in SiteScope alert templates.

Available Properties	Description / Example	Included in Templates
<_eventCategory>		NTEventlog
<_httpPort>		NTEventlog
<_webserverAddress>		NTEventlog
<alert>		XMLMail
<alertHelpURL>	URL of the SiteScope help including the alert topic	NoDetails Traceroute WithDiagnostic
<category>	The monitor category	Typical
<diagnostic>		XMLMail
<diagnosticText>		Default User NoDetails
<diagnosticTraceRoute>		Traceroute WithDiagnostic
<errorOnly>	Lists that monitor counters in error status	Typical
<eventID>		NTEventlog
<eventMachine>		NTEventlog
<eventSource>		NTEventlog
<eventType>		NTEventlog
<goodOnly>	Lists that monitor counters in good status	Typical

Available Properties	Description / Example	Included in Templates
<group>	Name of the group that the monitor is in	AllErrors Default Default User Ir-Default_mail_template NoDetails NTEventlogt PagerMail ShortMail Traceroute Typical WithDiagnostic XMLMail
<groupID>	ID of the group	Default Typical WithDiagnostic XMLMail
<id>		XMLMail
<mainParameters>	List of the main monitor properties that are set as parameter	Default Default User NTEventlog WithDiagnostic
<mainStateProperties>	List of main monitor properties that are set as state properties. These are the result statistics that are shown on the Reports.	Default Default User NTEventlog WithDiagnostic
<monitor>		XMLMail

Available Properties	Description / Example	Included in Templates
<name>	Name of the monitor (same as <code>_name</code> )	Default Default User lr-Default_mail_template NoDetails NTEventlog PagerMail ShortestMail ShortMail ShortSubject Traceroute Typical WithDiagnostic XMLMail
<newSiteScopeURL>	URL of the SiteScope server	Default Typical
<sample>	Sample #	AllErrors Default Default User NoDetails NTEventlog PagerMail ShortMail Traceroute Typical Typical.mail WithDiagnostic XMLMail
<server>		XMLMail



Available Properties	Description / Example	Included in Templates
<sitescope>		XMLMail
<sitescopeURL>		AllErrors Default User NoDetails Traceroute WithDiagnostic
<state>	Status string reported by the monitor (same as stateString)	AllErrors Default Default User Ir-Default_mail_template NoDetails PagerMail ShortestMail ShortMail ShortSubject Traceroute Typical WithDiagnostic XMLMail

Available Properties	Description / Example	Included in Templates
<tag>	Tags of the monitor (if exists)	Default Default User Ir-Default_mail_template NoDetails NTEventlog PagerMail ShortestMail ShortMail ShortSubject Traceroute Typical WithDiagnostic XMLMail
<time>	Time that the monitor completed the last run	AllErrors Default Default User Ir-Default_mail_template NoDetails NTEventlog Traceroute Typical WithDiagnostic XMLMail
<warningOnly>	Lists that monitor counters in warning status	Typical

## Additional General Template Properties

Available Properties	Description
<All>	All of the properties of the monitor
<alert::name>	The name of the alert
<alert::id>	The alert ID
<alert::description>	Text description for the alert definition
<alert::disableDescription>	Description of the purpose of the disable operation
<alert::actionID>	The ID for the alert action
<alert::actionName>	The name of the alert action
<bacMonitorID>	The monitor's Business Availability Center ID
<bacSessionID>	The Business Availability Center profileID
<currentTime>	The time that the alert is run
<GroupDescription>	Group description
<FullGroupId>	Full path from the SiteScope root directory to the group, exclude\SiteScope
<remoteMachineName>	The name of the remote server machine
<secondaryStateProperties>	Lists the main state properties and other internal properties
<time-date>	The date portion of the time that the monitor completed
<time-time>	The time portion of the time that the monitor completed

## Email Report Properties

The following properties are applicable to the email templates stored in the <SiteScope>\templates.history directory:


Available Properties	Description
_httpPort	Port number used to access SiteScope
_webserverAddress	IP address for the SiteScope Server
basicAlertSummary	Basic information on what alerts have been triggered
detailAlert Summary	More detailed information on alerts
reportIndexURL	URL to the index page for the management report
reportPeriod	Time period for this report
reportURL	URL to the HTML version of the management report
summary	Summary and measurement information
textReportURL	URL to the comma-delimited file generated by SiteScope
userReportIndexURL	URL to the index page for a user-accessible report
userTextReportURL	URL to the comma-delimited file generated by a user-accessible report
userXMLReportURL	URL to the XML file generated by a user-accessible report
xmlReportURL	URL to the XML file generated by the management report

## SiteScope Alerts User Interface



### This section includes:











- SiteScope Alerts Page on page 1997
- New/Edit Alert Dialog Box on page 1999
- Action Type Dialog Box on page 2006
- Alert Action Dialog Box - Action Type Settings Panel on page 2009

## SiteScope Alerts Page

<b>Description</b>	Displays information about the alerts associated with the selected monitor or group.  Use this page to add, edit, or delete alert definitions.  <b>To access:</b> Select a group or monitor in the monitor or template tree that has the alert symbol  displayed next to it. In the right pane, click the <b>Alerts</b> tab to display the alerts configured for the object.
<b>Important Information</b>	Alerts created for a specific monitor or group are displayed in the object's <b>Alerts on Monitor/Group</b> list. Targeted monitors or groups are displayed in the <b>Alerts Associated with Monitor/Group</b> list.
<b>Included in Tasks</b>	"Configure an Alert" on page 1984
<b>Useful Links</b>	"SiteScope Alerts Overview" on page 1960


The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click <b>Show Child Alerts to</b> display only those alerts that are direct children of the selected node.
	Click <b>Show All Descendent Alerts</b> to display all descendent alerts of the selected node.

GUI Element	Description
	<p>Click <b>New Alert</b> to open the New Alert dialog box which enables you to configure an alert, and add it to the selected SiteScope group or monitor. For details on the user interface, see “New/Edit Alert Dialog Box” on page 1999.</p> <p><b>Note:</b> This button is available in the <b>Alerts on Monitor/Group</b> table only</p>
	<p>Click <b>Edit Alert</b> to open the Edit Alert dialog box which enables you to edit the properties of the selected alert. For details on the user interface, see “New/Edit Alert Dialog Box” on page 1999.</p>
	<p>Click <b>Copy</b> to make a copy of the alert.</p> <p><b>Note:</b> This button is available in the <b>Alerts on Monitor/Group</b> table only.</p>
	<p>Click <b>Paste</b> to paste the alert to a selected location in the tree.</p> <p><b>Note:</b> This button is available in the <b>Alerts on Monitor/Group</b> table only.</p>
	<p>Click <b>Delete Alert</b> to delete the alert from the tree.</p>
	<p>Click <b>Enable</b> to enable the alert associated with the monitor/group.</p>
	<p>Click <b>Disable</b> to disable the alert associated with the monitor/group.</p>
	<p>Click <b>Test</b> to test the alert definition on a selected server.</p>
	<p>Click <b>Select All</b> to select all listed alerts.</p>
	<p>Click <b>Clear Selection</b> to clear the selection.</p>
<p><b>Name</b></p>	<p>The name by which the alert is known in SiteScope.</p>
<p><b>Status</b></p>	<p>The enabled/disabled status of the alert.</p>

GUI Element	Description
Description	A description of the alert.
Action Name	The name given to the alert action in the Action Type Dialog Box.

## New/Edit Alert Dialog Box

Description	<p>Enables you to define alerts for a SiteScope, a group, or a monitor.</p> <p><b>To access:</b> Right-click the SiteScope, group, or monitor for the alert, and select <b>New &gt; Alert</b>, or select an existing alert in the Alerts tab (monitor or template view) and click the <b>Edit Alert</b>  button.</p>
Important Information	Any box with a red asterisk (*) must be filled.
Included in Tasks	“Configure an Alert” on page 1984
Useful Links	<ul style="list-style-type: none"> <li>▶ “SiteScope Alerts Overview” on page 1960</li> <li>▶ “Action Type Dialog Box” on page 2006</li> <li>▶ “Alert Action Dialog Box - Action Type Settings Panel” on page 2009</li> </ul>

### General Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
Name	Enter a text description for this alert definition. This name is used to identify this alert definition in the product display.
Alert description	You can type free text to give a description to this alert. This description does not appear in any other context. It appears only when editing the alert.






## Alert Targets

The following elements are included (unlabeled GUI elements are shown in angle brackets>):













GUI Element	Description
<b>Alert targets</b>	<p>Use the context menu tree to select the groups and/or monitors to trigger this alert. The context menu includes the currently selected object and all of the child objects. Check the box beside the current object to associate this alert with all objects within this object. Check one or more individual objects to associate this alert definition to the selected objects.</p> <p>Alternatively, you may select the SiteScope root and then define an alert filter rule in the Filters Settings to limit alerting to those objects that match the conditions set in the filter.</p>

## Alert Actions

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click <b>New Alert Action</b> to open the Action Type dialog box, which enables you to define an action to be done when an alert is triggered. For details on the user interface, see “Action Type Dialog Box” on page 2006.
	Edits the alert action. For details on the user interface, see “Action Type Dialog Box” on page 2006.
	Deletes the alert action. It does not disable the associated monitors.
	Duplicates the alert action.
	Selects all listed alert actions.



GUI Element	Description
	Clears the selection.
 <Alert Action Type icon>	Indicates the type of action defined in the alert.
	 <b>Database.</b> Sends an alert message with a description of the problem as a record to a SQL database.
	 <b>Disable or Enable Monitors.</b> Manually controls the generation of alerts.
	 <b>Email.</b> Sends an email message to one or more email addresses with a description of the error or warning.
	 <b>Log Event.</b> Logs events to the Microsoft Windows Event Log.
	 <b>Pager.</b> Sends a message to a pager to signal that SiteScope has detected a particular condition.
	 <b>Post.</b> Submits a CGI POST containing a description of a monitor condition to a CGI script, servlet, or other CGI-enabled program.
	 <b>Script.</b> SiteScope can run scripts or batch files when the alert trigger condition is detected. The script or batch file that is called can run a system command or a program in any language that can be called from a command line entry.
	 <b>SMS.</b> Sends a short text message using the Short Message Service (SMS) to an SMS-enabled mobile phone or wireless device.
	 <b>SNMP Trap.</b> Sends an SNMP trap to an SNMP host or management console.
 <b>Sound.</b> Plays a sound or audio file on the machine on which SiteScope is running when an event has been detected.	
<b>Name</b>	The name given to the action to be done when the alert is triggered. It is not the name of the alert.

GUI Element	Description
<b>Category</b>	The category selected in the Status Trigger panel that triggers the alert action. For details on the Status Trigger user interface, see “Status Trigger Panel” on page 2024.
<b>When</b>	The schedule selected in the Trigger Frequency panel for when the alerts are sent. For details on the Trigger Frequency user interface, see “Trigger Frequency Panel” on page 2025.
<b>Schedule</b>	The daily or weekly schedule selected in the Action Type Settings panel. For details on the Action Type Settings panel user interface, see “Alert Action Dialog Box - Action Type Settings Panel” on page 2009.
<b>Target</b>	<p>Contains target data for the action type. Below you can see the content of the target column according to type:</p> <ul style="list-style-type: none"> <li>➤ Email. Contains the email recipients selected in the <b>Send email to</b> section.</li> <li>➤ Disable or Enable. Contains the targets selected in the <b>Targets</b> list.</li> <li>➤ Database. Contains the URL entered in the <b>Database connection URL</b> box.</li> <li>➤ Log Event. Contains the log event recipients selected in the <b>Send email to</b> section.</li> <li>➤ Pager. Contains the pager recipients selected in the <b>Pager Alert Recipients</b> list.</li> <li>➤ Post. Contains the URL entered in the <b>Post to url form</b> box.</li> <li>➤ Script. Contains the script selected in the <b>Script</b> box.</li> <li>➤ SMS. Contains the SMS number entered in the <b>SNMS number</b> box.</li> <li>➤ SNMP Trap. Contains the SNMP traps selected in the <b>SNMP Trap</b> list.</li> <li>➤ Sound. (The column is empty)</li> </ul>

## Enable/Disable Alerts

<b>Description</b>	Use to manually control the generation of alerts. This can be useful when the systems being monitored are off-line for maintenance or if the recipient of the alerts is unavailable for a period of time.
--------------------	---

The following elements are included (unlabeled GUI elements are shown in angle brackets):

<b>GUI Element</b>	<b>Description</b>
<b>Enable alert</b>	Overrides any disable action on the alert and enables the alert for execution based on the conditions defined.
<b>Disable alert indefinitely</b>	Prevents SiteScope from executing the alert action even if the alert condition is met until this radio button is cleared and the alert definition is updated.  <b>Note:</b> Use of this option may result in loss of expected alert capability if the alert is disabled to accommodate a temporary condition. It is important to review this status later to manually enable the alert definition, as needed.
<b>Disable alert for the next &lt;time period&gt;</b>	Prevents the execution of the alert action for the time period you type, even if the alert condition is met. The alerts are disabled immediately and re-enabled when the time period expires.
<b>Disable on a one time schedule from &lt;time1&gt; to &lt;time2&gt;</b>	Prevents SiteScope from executing the alert action for the time period indicated, even if the conditions are met. The alerts are disabled at the beginning of the time period and re-enabled after the time period expires.
<b>Disable description</b>	(Optional) Description of the purpose of the disable operation.

## Filter Settings

<b>Description</b>	<p>Creates filter conditions to limit the alert action to only those monitors that match the criteria you entered.</p> <p>You can define alerts for a large number of monitors and then apply a filter so that only certain monitors within the selected list actually trigger the alert. This can simplify the creation of alert definitions and alert management.</p>
<b>Important Information</b>	<p>To disable alert filtering, clear the applicable fields and update the alert definition.</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Name match</b>	<p>Suppresses the alert for all associated groups or monitors except those with a specific text appearing as part of their name.</p> <ul style="list-style-type: none"> <li>▶ Enter a regular expression in this text box to match a name string pattern. For details, see “Regular Expressions Overview” on page 262.</li> <li>▶ Enter all or part of the monitor name string you want to use as a filter criteria. For example, entering the string URL: limits this alert to monitors whose name contains the string URL:.</li> </ul> <p><b>Note:</b> The match is case sensitive.</p>



GUI Element	Description
<b>Status match</b>	<p>Suppresses the alert for all associated monitors except those returning a specific status text.</p> <ul style="list-style-type: none"> <li>▶ Enter a string that you expect to appear in the status text for the monitor you want to trigger this alert. For example, if you type the text <code>timeout</code>, an alert is only triggered by a monitor associated with this alert that also has a status of <code>timeout</code>.</li> <li>▶ Enter a regular expression in this text box to match a status string pattern. For details, see “Regular Expressions Overview” on page 262.</li> </ul> <p><b>Note:</b> The match is case sensitive.</p>
<b>Monitor type match</b>	<p>Limits the alert action to a monitor type from the set of monitors associated with this alert. Select the monitor types you want to include from the <b>Monitor Type List</b> and move them to the <b>Selected Monitor Type List</b> button.</p>

### Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>
<b>Add Tag</b>	<p>Click to add a new keyword tag.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>

## Action Type Dialog Box

<b>Description</b>	<p>Use the Action Type dialog box to select the action to be done when an alert is triggered.</p> <p><b>To access:</b> Right-click the SiteScope, group, or monitor for the alert, and select <b>New &gt; Alert</b>, or select an existing alert in the Alerts tab (monitor or template view) and click the <b>Edit Alert</b>  button. In the Alert Actions section of the New/Edit Alert dialog box, click the <b>New Alert Action</b>  button.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ You can select only one type of alert at a time.</li> <li>▶ If you are editing an alert, you cannot change the action type. For example, if an alert's action type was Email, you cannot change it to SMS.</li> </ul>
<b>Included in Tasks</b>	<p>“Configure an Alert” on page 1984</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Alerts Overview” on page 1960</li> <li>▶ “New/Edit Alert Dialog Box” on page 1999</li> <li>▶ “Alert Action Dialog Box - Action Type Settings Panel” on page 2009</li> </ul>



The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Database</b>	Sends an alert message with a description of the problem as a record to a SQL database. You can then use database tools to provide more advanced recording, sorting, and reporting on your monitoring data. For details on Database Alerts, see “Database Alert Properties” on page 2010.
<b>Disable or Enable Monitors</b>	Automatically enables or disables monitors or monitor groups based on a change of state in another monitor. <b>Note:</b> This action is not available when creating a template alert. For details on Disable/Enable Monitor Alerts, see “Disable or Enable Monitors Alert Properties” on page 2012.
<b>Email</b>	Sends an email message to one or more email addresses with a description of condition that triggered the alert. For details on Email Alerts, see “Email Alert Properties” on page 2013.
<b>Log Event</b>	Logs events to the Microsoft Windows Event Log. Entries in the event log can then be viewed with the Event Viewer and/or used by other software utilities that perform centralized alerting from the event log. For details on Log Event Alerts, see “Log Event Alert Properties” on page 2015.
<b>Pager</b>	Sends a message to a pager to signal that SiteScope has detected a particular condition. For details on Pager Alerts, see “Pager Alert Properties” on page 2016.
<b>Post</b>	Submits a CGI POST message to a CGI script, servlet, or other CGI-enabled program. The message contains a description of a monitor condition. For details on Post Alerts, see “Post Alert Properties” on page 2017.

GUI Element	Description
<b>Script</b>	<p>SiteScope can run scripts or batch files when the alert condition is met. The script or batch file can run a system command or a program in any language that can be called from a command line entry.</p> <p>You can use this alert to run recovery scripts that automatically respond to critical conditions or failures (for example, to reboot a server or to copy files). For details on Script Alerts, see “Script Alert Properties” on page 2019.</p>
<b>SMS</b>	<p>Sends a short text message using the Short Message Service (SMS) to an SMS-enabled mobile phone or wireless device. For details on SMS Alerts, see “SMS Alert Properties” on page 2021.</p>
<b>SNMP Trap</b>	<p>Sends an SNMP trap to an SNMP management console or host. This enables SNMP reporting of system parameters not normally supported by SNMP agents. For details on SNMP Trap Alerts, see “SNMP Trap Alert Properties” on page 2022.</p>
<b>Sound</b>	<p>Plays a sound or audio file on the machine on which SiteScope is running when an event has been detected. For details on Sound Alerts, see “Sound Alert Properties” on page 2023.</p>



## Alert Action Dialog Box - Action Type Settings Panel

<b>Description</b>	<p>Use the Alert Action dialog box to define the settings that are specific to the alert type and to configure actions to be taken when an alert is triggered.</p> <p>The Action Alert dialog box consists of three panels:</p> <ul style="list-style-type: none"> <li>▶ <b>Action Type Settings.</b> The Action Type settings vary according to the type of alert action you selected in the Action Type Dialog Box. For details, see the specific action type below.</li> <li>▶ <b>Status Trigger.</b> For details, see “Status Trigger Panel” on page 2024.</li> <li>▶ <b>Trigger Frequency.</b> For details, see “Trigger Frequency Panel” on page 2025.</li> </ul> <p><b>To access:</b> Right-click the SiteScope, group, or monitor for the alert, and select <b>New &gt; Alert</b>, or select an existing alert in the Alerts tab (monitor or template view) and click the <b>Edit Alert</b>  button. In the Alert Actions section of the New/Edit Alert dialog box, click the <b>New Alert Action</b>  button. In the Action Type dialog box, select an action type.</p> <p><b>Note:</b> When clicking the <b>Help</b> button in this dialog box, you may be prompted for your user login credentials.</p>
<b>Included in Tasks</b>	“Configure an Alert” on page 1984
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Alerts Overview” on page 1960</li> <li>▶ “New/Edit Alert Dialog Box” on page 1999</li> </ul>

The following element is common to all action types in the Action Type Settings:

GUI Element	Description
<b>Action name</b>	<p>The name given to the action to be done when the alert is triggered. It is not the name of the alert.</p> <p><b>Example:</b> If you want to configure an alert to check the CPU of all Solaris machines and send an SMS message when some alert is triggered, you could define the alert name in General Settings to be Solaris_CPU and the action name to be send_sms.</p>

### Database Alert Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Database connection URL</b>	<p>Enter the URL to a database connection.</p> <p><b>Example:</b> In Windows NT, use the ODBC Data Sources manager in the Settings control panel to create a connection called test and then type jdbc:odbc:test as the database connection URL.</p> <p><b>Note for using Windows Authentication:</b> If you want to access the database using Windows authentication, type jdbc:mercury:sqlserver://&lt;server name or IP address&gt;:1433;DatabaseName=&lt;database name&gt;;AuthenticationMethod=type2 as the connection URL, and com.mercury.jdbc.sqlserver.SQLServerDriver as your database driver. Leave the <b>Database user name</b> and <b>Database password</b> boxes empty, because the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.</p>

GUI Element	Description
<b>Database driver</b>	<p>Enter the Java class name of the JDBC database driver. SiteScope uses the same database driver for both primary and backup database connections. If a custom driver is used, the driver must also be installed in the <b>&lt;SiteScope root&gt;/java</b> directory. For more information about setting up database drivers for SiteScope, see “Database Query Monitor Overview” on page 477.</p>
<b>SQL statement</b>	<p>Enter the SQL statement used to add the alert to the database.</p> <p>Items enclosed in angle brackets (&lt; and &gt;) are replaced with fields from the monitor that triggered the alert.</p> <p><b>Default value:</b> INSERT INTO SiteScopeAlert VALUES('&lt;time&gt;', '&lt;group&gt;', '&lt;name&gt;', '&lt;state&gt;')</p>
<b>Database user name</b>	<p>Enter the user name to connect to the database if required.</p>
<b>Database password</b>	<p>Enter the password to connect to the database if required.</p>
<b>Backup database connection URL</b>	<p>If a backup database for SiteScope alert logging is required, enter the URL to the backup database connection to use if the main database connection fails.</p> <p><b>Example:</b> If the ODBC connection for the backup database connection is called testdb2, the URL would be jdbc:odbc:testdb2.</p>
<b>Schedule</b>	<p>Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered.</p> <p><b>Default value:</b> every day, all day</p>

## Disable or Enable Monitors Alert Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Group/Monitors action</b>	Select whether this alert action disables or enables a monitor when the alert is triggered. <b>Default value:</b> Disable
<b>Targets</b>	Select the groups and monitors that should be affected by the action of this alert. The <b>Targets</b> list includes all groups and monitors configured for the SiteScope. You can select any groups or monitors running in any group for this alert action and add them to the <b>Selected Targets</b> list. <b>Example:</b> This alert action is being configured for a Disk Space monitor. An alert triggered for this monitor can disable all CPU monitors monitoring the same server. <b>Default value:</b> None selected
<b>Schedule</b>	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. <b>Default value:</b> every day, all day

## Email Alert Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Send email to</b>	<p>Select email alert recipients using either of the following:</p> <ul style="list-style-type: none"> <li>▶ <b>Recipients.</b> Select one or more Email recipients for the alert from the Email Alert Recipients list. The list displays the recipients that have been configured in Mail Preferences. For details, see “Email Preferences” on page 1461.</li> <li>▶ <b>Addresses.</b> Enter one or more email addresses separated by a comma (","). The addresses are checked for valid syntax according to the official standard RFC 2822, but not for other errors (for example, that the email user exists).</li> </ul> <p><b>Note:</b> If the <b>Addresses</b> box contains data, selections from the Email Alert Recipients list are ignored.</p> <p><b>Default value:</b> None selected</p>
<b>Subject</b>	<p>Select the subject field template for the email alert action message. The Typical template includes the following values:</p> <ul style="list-style-type: none"> <li>▶ the subject of the message (SiteScope Alert)</li> <li>▶ the category of the monitor alert (error, warning, ok, or no data)</li> <li>▶ the name of the monitor or monitor title</li> <li>▶ the status returned by the monitor</li> <li>▶ the address, in parenthesis, of the SiteScope installation that sent the alert</li> </ul> <p><b>Default value:</b> Typical</p> <p><b>Example:</b> SiteScope Alert, error, URL: http://gate.company.com, unknown host name (gate.company.com)</p>

GUI Element	Description
<b>Template</b>	<p>Select the template for the email alert action.</p> <p>In an Email alert action, select the <b>ShortMail</b> template for a shorter email message. Other options enable you to choose the level of detail to include in Email alerts.</p> <p><b>Default value:</b> Typical. This template includes the following values: Monitor: &lt;groupID&gt;:&lt;name&gt;; Tags &lt;tag&gt;; Group: &lt;group&gt;; Status: &lt;state&gt;; Sample #: &lt;sample&gt;; Time: &lt;time&gt;</p> <p><b>Note:</b> You can add additional templates into the &lt;SiteScope root directory&gt;\templates.mail directory. For details on the available templates, you can open the files in this directory in a text editor to see what values are sent with each option.</p>
<b>Schedule</b>	<p>Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered.</p> <p>You cannot edit this value. It is determined by the schedule defined for the mail recipients in preferences.</p>
<b>Mark this action to close alert</b>	<p>When the status changes and the alert trigger condition is no longer true, this action closes the alert and sends a close notification by adding the word <b>Close</b> to the message sent.</p> <p><b>Default value:</b> Not selected</p>

## Log Event Alert Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Send to</b>	Enter the name of the Windows machine where the event is to be appended to the event log. <b>Default value:</b> localhost (the machine where SiteScope is running).
<b>Template</b>	Select the template for the log event type alert action. <b>Default value:</b> Typical <b>Note:</b> You can view the contents of the existing templates or add additional templates in <SiteScope root directory>\templates.eventlog.
<b>Message</b>	Enter the message prefix to be sent to the event log.
<b>Event source</b>	Enter the string used to set the <Source> field of the logged event. <b>Syntax:</b> must be text. <b>Default value:</b> SiteScope
<b>Event ID</b>	Enter the number used to set the <ID> field of the event that is logged. <b>Syntax:</b> must be numeric. <b>Default value:</b> 1000
<b>Event type</b>	Select the event type used for the event. <b>Default Value:</b> Use monitor status. This means that the Event Type is Error for an Error status, Warning for Warning, and Informational for monitors reporting a status of Good.
<b>Event category ID</b>	Enter a number to be used as the <category ID> for the event created by this alert. <b>Default value:</b> 0

GUI Element	Description
<b>Schedule</b>	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. <b>Default value:</b> every day, all day
<b>Mark this action to close alert</b>	When the status changes and the alert trigger condition is no longer true, this action closes the alert and sends a close notification by adding the word <b>Close</b> to the message sent. <b>Default value:</b> Not selected

### Pager Alert Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Pager alert recipients</b>	Select one or more pager recipients for the alert from the Pager Alert Recipients list. The list displays the recipients that have been configured in Pager Preferences. For details on this topic, see “Pager Preferences” on page 1471. <b>Default value:</b> None selected
<b>Template</b>	Select the template for the pager alert action type. <b>Default value:</b> Typical <b>Note:</b> You can view the contents of the existing templates or add additional templates in the <SiteScope root directory>\templates.page directory.
<b>Message</b>	Enter the message text to be sent to the pager. <b>Note:</b> The maximum length is 32 characters.



GUI Element	Description
<b>Schedule</b>	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered.  <b>Note:</b> You cannot edit this value. There is a predefined schedule for pager recipients defined in preferences.
<b>Mark this action to close alert</b>	When the status changes and the alert trigger condition is no longer true, this action closes the alert and sends a close notification by adding the word <b>Close</b> to the message sent.  <b>Default value:</b> Not selected

### Post Alert Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Post to URL form</b>	Enter the URL of the CGI script that SiteScope should submit to the alert. For example, <code>http://admindb.server.net/cgi-bin/error.pl</code> .  <b>Syntax:</b> You must include the string <code>http://</code> . There is syntax checking for a valid URL address.
<b>Template</b>	Select the template for the post alert action type.  <b>Default value:</b> Typical  <b>Note:</b> You can view the contents of the existing templates or add additional templates in the <code>&lt;SiteScope root directory&gt;\templates.post</code> directory.

GUI Element	Description
<b>Authorization user name</b>	<p>Enter the user name to access the URL of the CGI script in a Post Alert. Not all CGI scripts require a user name.</p> <p>Alternatively, leave this entry blank and type the user name in the <b>Default authentication user name</b> section in the General Settings (<b>Preferences &gt; General Preferences</b>). Use this method to define common authentication credentials for use with multiple monitors.</p>
<b>Authorization password</b>	<p>Enter the password for the Authorization user name in a Post Alert.</p> <p>Alternatively, leave this entry blank and type the password in the <b>Default authentication password</b> section in the <b>Preferences &gt; General Preferences</b>. Use this method to define common authentication credentials for use with multiple monitors.</p>
<b>HTTP proxy</b>	<p>Enter the domain name and port of an HTTP Proxy Server used to access the URL of the CGI script.</p>
<b>Proxy server user name</b>	<p>Enter the user name to access the URL of the CGI script, if required by the proxy server.</p> <p>Your proxy server must support Proxy-Authenticate.</p>
<b>Proxy server password</b>	<p>Enter the password to access the URL of the CGI script, if required by the proxy server.</p> <p>Your proxy server must support Proxy-Authenticate.</p>
<b>Schedule</b>	<p>Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered.</p> <p><b>Default value:</b> every day, all day</p>

## Script Alert Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Server</b>	<p>Select the server on which the script should be run.</p> <p>The scripts directory must be in the directory tree of the remote login account that allows remote scripts to be run by SiteScope.</p> <p><b>Default value:</b> SiteScope Server</p>
<b>Script</b>	<p>Select the script to run in response to the selected condition.</p> <p>You can create as many custom scripts as you need. Place them in &lt;SiteScope root directory&gt;\scripts directory or the applicable scripts directory on a remote machine. SiteScope lists all files found in this directory on the selected server in the drop-down list.</p> <p><b>Default value:</b> restartServer.bat</p>

GUI Element	Description
<b>Parameters</b>	<p>Additional monitor parameters that you can pass to your script, such as:</p> <ul style="list-style-type: none"> <li>➤ path of the scripts directory</li> <li>➤ name of the monitor that caused the alert</li> <li>➤ current status of the monitor</li> <li>➤ path to the alert message file</li> <li>➤ ID of the monitor</li> <li>➤ monitor group</li> </ul> <p>These parameters are sent as the seventh, eighth, ninth, and so forth, command line arguments respectively.</p> <p>The parameters available to be passed to the script are dependent on the type of monitor that triggers the alert.</p> <p><b>Syntax:</b> Surround the property name variable in the properties list with angle brackets (&lt; &gt;). For example, to pass the server name to the script, type &lt;_machine&gt; in the text box. To pass more than one extra parameter, separate the parameters with a single space. This is the same way the arguments would be added on the command line.</p> <p><b>Default value:</b> No value. The Script Alert always passes the above parameters to a script as command line arguments. They do not need to be listed here.</p>
<b>Output encoding</b>	<p>Select the encoding of the script output. This enables SiteScope to match and display the encoded file content correctly.</p> <p><b>Default value:</b> windows-1252</p>
<b>Template</b>	<p>Select the template for the script alert action type.</p> <p><b>Default value:</b> Typical</p> <p><b>Note:</b> You can view the contents of the existing templates or add additional templates in the &lt;SiteScope root directory&gt;\templates.script directory.</p>

GUI Element	Description
<b>Schedule</b>	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. <b>Default value:</b> every day, all day

### SMS Alert Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>SMS number</b>	Enter the telephone number required by the SMS service that identifies the destination for the message. <b>Syntax:</b> Numeric only. Maximum of 16 digits.
<b>Schedule</b>	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. <b>Default value:</b> every day, all day

## SNMP Trap Alert Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
SNMP Trap	Select one or more SNMP Traps to trigger an alert. <b>Default value:</b> None selected
Template	Select a template for the SNMP trap alert action type. Each line in the template is sent as a separate SNMP variable. The template file can also be modified using: <ul style="list-style-type: none"> <li>➤ [Agent Host: &lt;hostname-or-ip-address&gt;] as the first line of the template, to send the trap with that hostname or IP address as the source of the trap. By default, the IP address of the machine that SiteScope is running on is used as the source of the trap.</li> <li>➤ [Command: &lt;command name&gt;] to override the default command.</li> <li>➤ [Type: &lt;var-type&gt;] to override the default type of the object.</li> </ul> [OID: <object id>] to change the default object id. For example, use this to change a var-binding variable object id. <b>Default value:</b> Typical <b>Note:</b> You can view the contents of the existing templates or add additional templates in the <SiteScope root directory>\templates.snmp directory.
Message	Enter an optional prefix to be added to the SNMP trap sent by this alert.

GUI Element	Description
<b>Schedule</b>	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. <b>Default value:</b> every day, all day
<b>Mark this action to close alert</b>	When the status changes and the alert trigger condition is no longer true, this action closes the alert and sends a close notification by adding the word <b>Close</b> to the message sent. <b>Default value:</b> Not selected

### Sound Alert Properties

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Sound file</b>	Select the sound to be played from <code>&lt;SiteScope root directory&gt;\templates.sound</code> directory. Additional sounds can be added to the directory in AU format (8 bit, 16-bit, 8000 Hz, one-channel) with an .au suffix. <b>Default value:</b> Default
<b>Schedule</b>	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. <b>Default value:</b> every day, all day

 **Status Trigger Panel**

<b>Description</b>	Use the Status Trigger panel to select the status of the object type that triggers an alert action. Alerts are triggered when the status changes from one state to another. Select the category that triggers the alert action. <b>Default value:</b> Error
--------------------	--

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

<b>GUI Element</b>	<b>Description</b>
<b>Unavailable</b>	Alerts are triggered if the monitored machine was previously available and is currently no longer available.
<b>Error</b>	Alerts are triggered if the monitor was previously reporting a status of Good.
<b>Warning</b>	Alerts are triggered if the monitor was previously reporting a status of Good.
<b>Good</b>	Alerts are triggered if the monitor was previously reporting a status of Error.



## Trigger Frequency Panel

<b>Description</b>	Use the Trigger Frequency panel to select the trigger frequency.
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The available options vary according to what you chose in the Status Trigger Panel.</li> <li>▶ For more detailed information on the options here, see “Understanding When SiteScope Alerts Are Sent” on page 1964.</li> </ul>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Escalate, after action &lt;&gt; occurred exactly &lt;N&gt;times</b>	<p>Select this option if the alert action you are creating is dependent on another alert action. You must select the name of the alert action on which this alert action is dependent and the number of times the first alert action is triggered before this alert action is triggered.</p> <p><b>Example:</b> You created an alert action to send a sound alert when a certain condition is met. You want an Email alert to be sent when the sound alert action has been triggered 3 times. Select the name of the sound alert action and 3.</p> <p><b>Note:</b> This option is displayed only if another alert action has been defined for the alert.</p>
<b>Always, after the condition has occurred at least &lt;N&gt; times</b>	<p>After the alert conditions have occurred at least N times, the alert is triggered every time the alert conditions are met again after the initial trigger.</p> <p>Enter the minimum number of times the alert condition must be met before the alert is triggered the first time.</p> <p><b>Syntax:</b> numeric only</p> <p><b>Range:</b> 1-99</p>

GUI Element	Description
<p><b>Once, after the condition has occurred exactly &lt;N&gt; times</b></p>	<p>The alert is triggered only once after the alert condition is met for the Nth time.</p> <p>Enter the number of times the alert conditions must be met before the alert is triggered.</p> <p><b>Default value:</b> Selected</p> <p><b>Syntax:</b> numeric only</p> <p><b>Range:</b> 1-99</p>
<p><b>Initially after &lt;X&gt; times, and repeat every &lt;Y&gt; times</b></p>	<p>The alert is triggered after the alert condition occurs X consecutive times, and then the alert is triggered every consecutive Y occurrences that the alert conditions are met. For example, if X is set to 3, and Y is set to 4, then the alert action would be done on the 3rd, 7th, 11th, and so forth, occurrences of the alert condition.</p> <p><b>Syntax:</b> numeric only</p> <p><b>Range:</b> 1-99</p>
<p><b>Once, after &lt;N&gt; group errors</b></p>	<p>This is displayed if you chose <b>Error</b> in the Status Trigger panel.</p> <p>The alert is triggered only after any monitor in the group has reported the alert condition exactly N consecutive times.</p> <p><b>Note:</b> This option is available only for SiteScope groups.</p>

GUI Element	Description
<p><b>Once, after all monitors in this group are in error</b></p>	<p>This is displayed if you chose <b>Error</b> in the Status Trigger panel.</p> <p>The alert is triggered the first time all monitors in the group are in error.</p> <p><b>Note:</b> This option is available only for SiteScope groups.</p>
<p><b>Only alert if monitor was previously in error/warning at least &lt;N&gt; times</b></p>	<p>This is displayed if you chose <b>Good</b> or <b>Warning</b> in the Status Trigger panel.</p> <p>This option suppresses the triggering of the alert until the subject monitor or group has reported a status of either of the following:</p> <ul style="list-style-type: none"> <li>➤ <b>Error</b> or <b>Warning</b> for alert category <b>Good</b></li> <li>➤ <b>Good</b> or <b>Error</b> for alert category <b>Warning</b>, for at least the number of times that you entered</li> </ul>



## Writing Scripts for Script Alerts

This chapter includes information about how to write automated system recovery scripts for use with the SiteScope Script Alert.

### **This chapter includes:**

#### Concepts

- Writing Scripts for Script Alerts Overview on page 2029
- Working with Scripts in SiteScope on page 2030
- Passing Data from SiteScope to a Script on page 2032

### **Writing Scripts for Script Alerts Overview**

SiteScope has the ability to run scripts or batch files when an error or warning status is detected. This is normally done by creating a Script Alert that acts as a trigger for the script. The script or batch file can run any system command or call other programs written in any language. You can use this to create recovery scripts to automatically respond to critical conditions or failures.

## Working with Scripts in SiteScope

The script file that a SiteScope Script alert is to run must be located in the **<SiteScope root directory>\scripts** folder or on a remote UNIX machine (for remote scripts). For example, if SiteScope is installed in the directory C:\SiteScope and your script is called actionTest.bat, SiteScope tries to run the following command line in response to Script Alerts you have created:

```
C:\SiteScope\scripts\actionTest.bat C:\SiteScope\scripts monitor_name
```

where C:\SiteScope\scripts is the first command line parameter, monitor\_name is the second command line parameter, and so forth.

---

**Note:** While the local script run by the Script Alert must reside in **<SiteScope root directory>\scripts**, the execution path is **<SiteScope root directory>\classes** directory. You should use full paths for any file system commands or programs called by the script to avoid problems with defining the current execution directory.

---

The action taken by a script is determined by the creator of the script. SiteScope passes several command line arguments to each script called by a Script Alert. You can use this to have program scripts take action based on information sent from SiteScope. By default, SiteScope passes the following parameters to each Script alert as command line arguments:

- The path of the scripts directory.
- The name of the monitor that caused the alert.
- The current status of the monitor.
- The path to the alert message file.
- The Id code of the monitor.
- The group in which the monitor is located.
- Any additional parameters specified in the **Parameters** box in the alert form.

These command line arguments can be accessed by the target script using the normal command line variable conventions. These conventions are %1, %2, %3 and so forth, for Windows NT systems, and \$1, \$2, \$3 and so forth, for UNIX scripts (depending on the scripting shell or language used). The first six parameters (that is, %1 through %6) are passed by default to each script. To pass other parameters, the property variables or parameters must be added to the Script Alert Settings in the Parameters box to make them available to the script. The first variable or text entered in the Parameters box is then accessible as %7 by the script, the second parameter is accessed as %8, and so forth.

An example script written in Perl to access Script Alert parameters:

```
print "pathname to scripts directory: $ARGV[0]\n";
print "name of monitor causing alert: $ARGV[1]\n";
print "current status monitor: $ARGV[2]\n";
print "pathname to alert message file: $ARGV[3]\n";
print "id code of monitor: $ARGV[4]\n";
print "group for the monitor: $ARGV[5]\n";
```

The following is an example batch file for Microsoft Windows to echo the parameters passed to the script:

```
echo pathname to scripts directory: %1
echo name of monitor causing alert: %2
echo current status monitor: %3
echo pathname to alert message file: %4
echo id code of monitor: %5 echo group for the monitor: %6
```

## Passing Data from SiteScope to a Script

In addition to the seven default parameters, there are two other mechanisms for passing parameters and data to scripts. One is to use the additional Parameters box in the Script Alert Settings. The other is to access the Alert Message file.

This section includes the following topics:

- ▶ “Passing Data Using the Script Alert Settings” on page 2032
- ▶ “Passing Data Using the Alert Message File” on page 2033

### Passing Data Using the Script Alert Settings

The simplest way to send additional custom parameters and data to script is to use the Alert Action dialog box. The seventh default parameter passed to the script, which is any additional parameters specified on the alert form, allows you to specify one or more custom parameters to be sent to the script. You specify these for a Script Alert in the **Parameters** box on the Action Types Settings panel of the Alert Action dialog box.

These parameters could be hard-coded values. You can include multiple parameters by separating the individual parameters by spaces. For example, assume you want to pass the four text strings shown below to a script. To do this you type them in the Parameters box as follows:

Parameters	customAcustomBcustomCcustomD
------------	------------------------------



These would then become the seventh (7th) through tenth (10th) command line parameters sent to the script. The following Windows batch file script would print the default parameters as well as the additional example custom parameters entered in the Parameters box of the Action Types Settings Page:

```
echo pathname to scripts directory: %1
echo name of monitor causing alert: %2
echo current status monitor: %3
echo pathname to alert message file: %4
echo id code of monitor: %5
echo group for the monitor: %6
echo seventh parameter(customA): %7
echo eighth parameter(customB): %8
echo ninth parameter:(customC) %9
echo tenth parameter(customD): %10
```

## Passing Data Using the Alert Message File

The other method for passing data and SiteScope monitor parameters to a script is to use the Alert Message file. This is a file that is created by SiteScope using the alert template specified in the Alert Action dialog box. You can create your own custom alert templates and pass custom text strings or any of the SiteScope parameters available. The following shows the default NTEventLog template included with SiteScope. The parameters marked with < > brackets are replaced with the applicable values to and written to the Alert Message file each time the applicable Script Alert is triggered.

```
The NTEventLog Script Alert Template
Type: <eventType>
Event Time: <eventTime>
Source: <event>
Source ID: <eventID>
Category: <eventCategory>
Machine: <eventMachine>
Message: <eventMessage>
Monitor: <name>
Group: <group>
Sample #: <sample>
Time: <time>
<mainParameters>
<mainStateProperties>
```

To use this data in a script, your script needs to access the Alert Message file at the pathname location specified by the fourth default command line parameter (see “Working with Scripts in SiteScope” on page 2030). Then the script has to parse the content of the Alert Message file to extract the data you want to use in your script.

For more examples of how to write recovery scripts, look at the script files in the <SiteScope root directory>\scripts directory. You can use the **actionTest.bat** example template to create your own script. The **perlTest.pl** example shows how to call a Perl script. The **restartIIS.bat**, **restartService.bat**, and **restartServer.bat** scripts implement common recovery actions.

For the UNIX environment, the examples scripts are called action **Test.sh** and **perlTest.pl**.

---

## SiteScope Reports

This chapter includes the main concepts, tasks, and reference information for SiteScope reports.

### **This chapter includes:**

#### Concepts

- ▶ SiteScope Reports Overview on page 2035
- ▶ SiteScope Report Types on page 2037
- ▶ Working with SiteScope Management Reports on page 2039

#### Tasks

- ▶ Create a Report on page 2041

#### Reference

- ▶ SiteScope Reports User Interface on page 2042

### **SiteScope Reports Overview**

SiteScope reports display information about how the servers and applications you are monitoring have performed over time. SiteScope reports are important tools in monitoring and troubleshooting operational performance and availability and reviewing the monitored environment.

You can create a report for a single monitor, several monitors, or even a number of monitor groups. Report definitions include report content options such as tables of specific monitor measurements, summaries of results, and graphs.

SiteScope reports can be valuable to many people in your organization, including management personnel in Sales, Marketing, Customer Support, and Operations. SiteScope User accounts can be created to enable these users restricted access to the SiteScope service to view reports. For more information, see “User Management Preferences Overview” on page 1498.

---

**Note:**

- ▶ To view certain report elements on SiteScope for UNIX/Linux, it is necessary that an X Window system be running on the server where SiteScope is running.
  - ▶ To be able to open reports generated in SiteScope version 9.0 and later after upgrading the SiteScope installation, you should create a manual backup of the reports folder <SiteScope root directory>\htdocs, and copy it to the new installation directory.
- 

## SiteScope Monitor Data Log Files

SiteScope monitor data available for generating reports is limited to the amount of log data stored on the SiteScope server. By default, SiteScope retains monitor data log files for 40 days. The log files are rotated and files older than the log retention period are automatically deleted.

---

**Note:** Keeping monitor data logs for longer periods can cause a data storage problem for the SiteScope server depending on the total number of monitors configured and how often the monitors run per day. You should monitor the size of log files in the <SiteScope root directory>\logs directory to estimate the data accumulation rate.

---

You can change the length of time that SiteScope retains monitor data using the log preferences. You can configure SiteScope to export monitor data to an external SQL-compliant database to maintain monitor data for longer periods or to make the data available to other reporting applications. For details, see “Log Preferences Overview” on page 1449.


## SiteScope Report Types

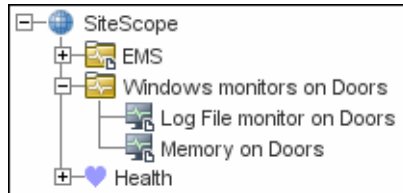
SiteScope includes four kinds of management reports. The following describes the report types and their usage.

Report Type	Description
<b>Alert Reports</b>	<p>Alert reports provide information about SiteScope alerts generated during a specified period of time. You create an Alert report on an ad hoc basis. In addition, the settings for an Alert report are not saved to the SiteScope configuration data for later use.</p> <p>For details on configuring the Alert report, see “New SiteScope Alert Report Dialog Box” on page 2070.</p>
<b>Management Reports</b>	<p>Management reports provide a summary of infrastructure availability and performance data for a given period of time. Management reports are generated automatically based on their preset schedule from data collected by SiteScope monitors. According to the preset schedule, SiteScope reads the applicable log files and generates the report based on the monitor metrics for the time interval specified. You can save the report data in a file suitable for exporting to third-party applications.</p> <p>For details on configuring the Management report, see “New/Edit SiteScope Management Report Dialog Box” on page 2045.</p>
<b>Monitor Reports</b>	<p>Monitor reports enable you to review configuration properties and settings for existing monitors. You can export a monitor report in one of three text data formats. Unlike a Management report which is based on a schedule that you specify, you create a Monitor report on an ad hoc basis. In addition, the settings for a Monitor report are not saved to the SiteScope configuration data for later use.</p> <p>For details on configuring the Monitor report, see “New SiteScope Monitor Report Dialog Box” on page 2067.</p>

Report Type	Description
<p><b>Quick Reports</b></p>	<p>Quick reports enable you to view monitor data for specific monitors or groups of monitors during specific time periods.</p> <p>Unlike a Management report that is generated based on a schedule that you specify, you create a Quick report on an ad hoc basis. In addition, the settings for a Monitor Summary report are not saved to the SiteScope configuration data for later use.</p> <p>For details on configuring the Quick report, see “New SiteScope Quick Report Dialog Box” on page 2060.</p>
<p><b>BAC Configuration Changes Report</b></p>	<p>Displays statistics about the configuration reporting to HP Business Availability Center. It should be used for troubleshooting purposes only.</p> <p>The report is generated from HP Business Availability Center. If there are multiple SiteScopes reporting to HP Business Availability Center, the information displayed in this report includes information not only for the specific SiteScope selected.</p> <p><b>Example:</b> The report logs exceptions, such as a failure to enter data into the profile database.</p> <p><b>Note:</b> The report is available only when accessing SiteScope from System Availability Management Administration and if the user has permission to view SiteScope logs.</p>

## Working with SiteScope Management Reports

Reports are added as elements to the Reports tab in the monitor view. They can be added as a child to the SiteScope node, to a group, or to an individual monitor. Reports are displayed in the left menu tree by a  icon next to the group or monitor for which it was created, as shown in the example below.



Reports have a scope based on the container to which they are added. You add a report to the container or element that contains all of the monitors whose data you want to include in the report. You then use the **Report Targets** panel to narrow the selection of monitors to be included in the report.

When you select a node with a report icon, the Report tab displays two tables. The **Reports on** table displays the reports created on this node. The **Reports Associated with** table displays the reports created on an ancestor node and applied to this node using the target selection.

You can create as many SiteScope report definitions as you want. However, you should plan and consolidate reports to keep the number of report definitions to a minimum. This can facilitate report administration and help reduce redundant report messages or actions. When creating a report for a large number of monitors, you should consider making separate reports based on the type of monitor or measurement. For example, when reporting on system resources for 20 different remote servers, consider making one report with monitors that measure numeric values such as CPU or disk space and another report for monitors that report basic availability such as services or processes.

By default, SiteScope keeps the 10 most recently generated reports. This means that hourly reports are available for the last 10 hours, daily reports are available for 10 days, weekly reports are available for 10 weeks, and so forth. You can change this report storage period by changing the value of the `_maximumReports` setting in the SiteScope `master.config` file.

Deleting a Management report definition discontinues the generation of applicable report. Previously generated reports continue to be available until the underlying data is removed.

You can copy and paste a report definition. The report definition settings are pasted to the new location with the exception of the **Report targets** setting, which are automatically reset to include all of the children of the container into which the report is pasted. After pasting a report, you should edit the report definition properties to be sure that the assigned **Report targets** are appropriate to the new report context and your overall reporting plan.



## Create a Report

This task describes the steps involved in creating a SiteScope report.

This task includes the following steps:

- “Select a Report Type” on page 2041
- “Configure the Report Settings” on page 2041
- “Results” on page 2042

### 1 Select a Report Type

Right-click the group or monitor container in which you want to create a report, and click **Reports**, or create a new report from the Reports tab. Select the report type you want to add or generate (only the Management report is added; all other reports are ad hoc and are not saved in SiteScope).

For details of report types, see “SiteScope Report Types” on page 2037.

### 2 Configure the Report Settings

Select the monitors to include in the report and configure the report settings.


For details on the report settings user interface, see “SiteScope Reports User Interface” on page 2042.

---

**Note:** By default, a report includes data from all monitors within the selected container. For Alert Reports, you cannot remove any of the monitors in the selected container from the report.

---

### 3 Results

Management reports are added to the selected container in the monitor tree (indicated by a report  symbol). For details on viewing the Management report, see “Management Report” on page 2072.

All other reports are generated and displayed in your Web browser.


- ▶ For details on viewing the Alert report, see “Alert Report” on page 2083.
- ▶ For details on viewing the Monitor report, see “Monitor Summary Report” on page 2080.
- ▶ For details on viewing the Quick report, see “Quick Report” on page 2076.

## SiteScope Reports User Interface



### **This section includes:**









- ▶ Reports Page on page 2043
- ▶ New/Edit SiteScope Management Report Dialog Box on page 2045
- ▶ New SiteScope Quick Report Dialog Box on page 2060
- ▶ New SiteScope Monitor Report Dialog Box on page 2067
- ▶ New SiteScope Alert Report Dialog Box on page 2070
- ▶ Management Report on page 2072
- ▶ Quick Report on page 2076
- ▶ Monitor Summary Report on page 2080
- ▶ Alert Report on page 2083
- ▶ Annotation Tool on page 2085

## Reports Page

<b>Description</b>	<p>Displays information about the reports defined in SiteScope.</p> <p>Use this page to add, edit, or delete report definitions.</p> <p>If a report has been set up for a SiteScope object (group or monitor), the report symbol  is displayed next to the object icon in the monitor tree. Select the SiteScope object to display report properties for the specific object.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, click the <b>Reports</b> tab.</p>
<b>Important Information</b>	<p>Reports created for a specific monitor or group are displayed in the object's <b>Reports on Monitor/Group</b> list. Targeted monitors or groups are displayed in the <b>Reports Associated with Monitor/Group</b> list.</p>
<b>Included in Tasks</b>	<p>"Create a Report" on page 2041</p>
<b>Useful Links</b>	<p>"Working with SiteScope Management Reports" on page 2039</p>

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
	Click <b>Show Child Reports</b> to display only those reports that are direct children of the selected node.
	Click <b>Show All Descendent Reports</b> to display all descendent reports of the selected node.

GUI Element	Description
	<p>Click the <b>New Report</b> button, and select the type of report you want to configure. Only Management reports are added to the Reports tab (all other report types are created on an ad hoc basis, and are not saved in SiteScope). For details on the New SiteScope Management Report user interface, For details on the user interface, see “New/Edit SiteScope Management Report Dialog Box” on page 2045.</p> <p><b>Note:</b> This button is available in the <b>Reports on Monitor/Group</b> table only.</p>
	<p>Click the <b>Edit Report</b> button to edit the properties of the selected Management report. For details on the Edit SiteScope Management Report user interface, see “New/Edit SiteScope Management Report Dialog Box” on page 2045.</p>
	<p>Click the <b>Copy Report</b> button to make a copy of the selected report.</p> <p><b>Note:</b> This button is available in the <b>Reports on Monitor/Group</b> table only.</p>
	<p>Click the <b>Paste Report</b> button to paste the report to the selected location in the tree.</p> <p><b>Note:</b> This button is available in the <b>Reports on Monitor/Group</b> table only.</p>
	<p>Click the <b>Delete Report</b> button to delete the selected Management report from the Reports tab.</p>
	<p>Click the <b>Generate Report</b> button to generate a Management report for a selected monitor or group. For details on the user interface, see “Management Report” on page 2072.</p>
	<p>Click the <b>Select All</b> button to select all listed reports.</p>
	<p>Click the <b>Clear Selection</b> button to clear the selection.</p>
<p><b>Type</b></p>	<p>Indicates the report type.</p>

GUI Element	Description
<b>Title</b>	The name by which the report is known in SiteScope.
<b>Description</b>	A description of the report.
<b>Enabled</b>	Indicates whether the generation of this report is enabled.
<b>Path</b>	Displays a link to the ancestor node that is targeting this object.  <b>Note:</b> This column is available in the <b>Reports associated with table</b> only.

## **New/Edit SiteScope Management Report Dialog Box**

<b>Description</b>	Enables you to create a report that provides a summary of system availability data for a given time period.  <b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor, and select <b>Reports &gt; Management</b> .
<b>Important Information</b>	HTML code entered in report text boxes is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected. The following is prohibited HTML content:  <ul style="list-style-type: none"> <li>▶ Tags: <b>script</b>, <b>object</b>, <b>param</b>, <b>frame</b>, <b>iframe</b>.</li> <li>▶ Any tag that contains an attribute starting with <b>on</b> is declined. For example, <b>onhover</b>.</li> <li>▶ Any attribute with <b>javascript</b> as its value.</li> </ul>
<b>Included in Tasks</b>	“Create a Report” on page 2041
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Reports Overview” on page 2035</li> <li>▶ “Reports Page” on page 2043</li> <li>▶ “Management Report” on page 2072</li> </ul>

## General Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Report title</b>	Enter a title for this Management Report. This name is used to identify this Management Report definition in the product display.
<b>Description</b>	(Optional) Use this text box to describe other information about this report definition. For example, include information about the purpose, target, setup date, or audience for this report.

## Report Targets

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Report targets</b>	Select the groups and/or monitors to be included in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers.  <b>Default value:</b> The current container and all child elements are selected.

## Display Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Thresholds</b>	
<b>All thresholds</b>	Creates a table of monitor error, warning, and good threshold settings for all of the monitors included in the report. If selected, this table is displayed as the first report section. <b>Default value:</b> Not selected
<b>Error thresholds</b>	Creates a table of individual error readings recorded by the monitors during the report period. <b>Default value:</b> Selected
<b>Warning thresholds</b>	Creates a table of individual warning readings recorded by the monitors during the report period. <b>Default value:</b> Selected
<b>Good thresholds</b>	Creates a table of individual good readings recorded by the monitors during the report period. <b>Default value:</b> Selected
<b>Uptime and Readings</b>	
<b>Uptime Summary and Measurement Summary tables</b>	Creates two report tables: <b>Uptime Summary</b> and <b>Measurement Summary</b> . For details of the data included in these tables, see "Report Content - Management Report Page" on page 2074. <b>Default value:</b> Selected
<b>Uptime: Include warnings</b>	Includes any monitor readings that are reported as warnings in the overall Uptime calculation. <b>Default value:</b> Not selected

GUI Element	Description
<b>Uptime: Ignore warnings</b>	<p>Suppresses monitor readings reported as warnings from the overall Uptime and Readings Summary section.</p> <p><b>Note:</b> This option only suppresses the display of the Warning % column in the table; it does not change the calculation of the Uptime %.</p> <p><b>Default value:</b> Not selected</p>
<b>Uptime: Ignore errors</b>	<p>Suppresses monitor readings reported as errors from the overall Uptime and Readings Summary section.</p> <p><b>Note:</b> This option only suppresses the display of the Error % column in the table; it does not change the calculation of the Uptime %.</p> <p><b>Default value:</b> Not selected</p>
<b>General</b>	
<b>Measurements graph</b>	<p>For graph reports, use the drop-down list to choose a graphical measurement to be included in the report. For details of the options, see “Graph Measurement Options” on page 2058.</p>
<b>Monitor readings</b>	<p>Creates a table of individual readings recorded by the monitors during the report period, including all readings (error, good, and warning). This report table may also include blank "buckets" depending on the period of the report and how often the monitors ran during the period.</p> <p><b>Default value:</b> Selected</p>



GUI Element	Description
<p><b>Alerts table</b></p>	<p>Select an option to include a table of alerts sent for the monitors in the report. The options for the alerts table level are:</p> <ul style="list-style-type: none"> <li>▶ <b>No alerts table.</b> No table of alerts is included in the report (default)</li> <li>▶ <b>Basic alerts table.</b> Displays the time and summary information for each alert sent.</li> <li>▶ <b>Show detailed alerts table for all alerts.</b> Displays detailed alert information for each alert in the report.</li> <li>▶ <b>Show detailed alerts table for failed alerts.</b> Displays the time and summary information for each alert, and a full diagnostics breakdown for each failed alert.</li> </ul>
<p><b>Detailed monitor information</b></p>	<p>Displays all of the information gathered for each monitor on the report. Otherwise, only the primary data is displayed for each monitor.</p> <p><b>Default value:</b> Not selected</p> <p><b>Example:</b> If this box is checked on a URL Sequence Monitor, the timing information for each step in the sequence is displayed in the report.</p>
<p><b>Time in error</b></p>	<p>Creates a table summary listing each monitor selected for the report with a summary of how many minutes the monitor status was calculated as being in error for the period of the report.</p> <p><b>Default value:</b> Not selected</p>

## Filter and Scheduling Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Monitor filter</b>	<p>Select a subset of those monitors to be shown in the report—those that have had the specified status sometime during the report's time frame. You can select only monitors in error or warning, monitors in error, monitors in warning, monitors that were OK, or all monitors.</p> <p><b>Default value:</b> Show all monitors</p> <p><b>Example:</b> Choosing <b>Show only monitors in error</b> displays report data only if that monitor had spent time in error sometime during the time interval of the report.</p>
<b>Schedule filter</b>	<p>Select a schedule filter option for showing only a subset of the data in the report—those monitors that have samples during the time period of the schedule.</p> <p><b>Default value:</b> The report shows data for the full period of the report (every day, all day).</p> <p><b>Example:</b> Choosing weekdays, 09:00-18:00 displays report data for the selected monitors with samples from the 9am to 6pm time period, Monday through Friday. Only this data is used for all the calculations.</p>

GUI Element	Description
<b>Time period for report</b>	<p>Select the time period for which you want to view monitoring data. You can choose to report on data for a set number of hours, for the last day, the last several days, the past week, past month, or month-to-date for the current calendar month.</p> <p><b>Default value:</b> Last day</p> <p><b>Note:</b> Daily and month-to-date reports are generated every day at the scheduled time. Weekly reports are generated on Sundays at the scheduled time, and monthly reports are generated on the first day of the month following the current month so that they contain an entire month's worth of data.</p>
<b>End of report period</b>	<p>Choose an end time for the report by selecting a time from the drop-down list. For example, you may want to have your reports run from midnight to midnight.</p> <p><b>Default value:</b> At time report is run (SiteScope generates reports starting at the indicated time and ending at the time the report was generated)</p>

## Report Format

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>File format</b>	<p>This option enables some customization of the report appearance. The options are:</p> <ul style="list-style-type: none"> <li>➤ <b>Color background</b> (default)</li> <li>➤ <b>Color background, no table borders</b></li> <li>➤ <b>White background</b></li> </ul>

## Report Distribution

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>HTML format</b>	<p>Select if you want the reports sent in HTML format. Use this option to include the SiteScope report graphics. If you do not select this option only a text summary of the report is sent.</p> <p><b>Default value:</b> Not selected</p>
<b>Send report to email address</b>	<p>To have the report forwarded by email when it is generated, enter the email address(es) to which this report should be sent each time its generated. To send the reports to multiple email addresses, separate the email addresses with commas.</p>
<b>Format template</b>	<p>Select a template for SiteScope to use to create the email message. You can choose from the following templates or make a copy of one of these and customize it to meet your own needs.</p> <ul style="list-style-type: none"> <li>➤ <b>HistoryLongMail</b> - Choose this option to send a detailed history report. It contains both user and administration links.</li> <li>➤ <b>HistoryLongXMLMail</b> - Choose this option to send a detailed history report. It contains both user and administration links for reports &amp; XML files.</li> <li>➤ <b>HistoryMail</b> - Choose this option to send a history report. This is the default option.</li> <li>➤ <b>HistoryMailAlertDetail</b> - Choose this option to have all alerts included in the report that is sent by email.</li> <li>➤ <b>HistoryMailNoLinks</b> - Choose this option to send the report without any links in it.</li> </ul>

GUI Element	Description
<p><b>Comma-delimited file</b></p>	<p>Select to save a generated management report to a comma-delimited text file which you can then import into a spreadsheet application.</p> <p>SiteScope automatically saves these files in the <b>&lt;SiteScope root directory&gt;\htdocs</b> directory. To find the exact location of the saved file on your machine, click the <b>View Report</b> tab for the report, and move the pointer over the <b>text</b> link for the report in the <b>Information For</b> column. The full path to the file is listed in the status bar of your Web browser. To open the saved file on your machine, click the <b>text</b> link to go to the Report page. If you enter an email address in the <b>Email</b> text box, SiteScope sends a copy of the comma-delimited file to that address.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> The comma-delimited file creates two columns for each monitor reading; one containing the value with units, and the other containing just the value. This is to make it easier to import the comma-delimited data into a third party application which may not automatically separate data values from the text describing the units.</p>
<p><b>Send comma-delimited file by email</b></p>	<p>If you enter an email address in the text box, SiteScope sends a copy of the file to that address.</p>

GUI Element	Description
<b>XML file</b>	<p>Select this box to save a generated management report to an XML text file. SiteScope automatically saves these files in the &lt;SiteScope root directory&gt;\htdocs directory. To find the exact location of the saved file on your machine, click the <b>View Report</b> tab for the report, and move the pointer over the <b>xml</b> link for the report in the <b>Information For</b> column. The full path to the file is listed in the status bar of your Web browser. To open the saved file on your machine, click the <b>xml</b> link to go to the Report page. If you enter an email address in the <b>Email</b> text box, SiteScope sends a copy of the comma-delimited file to that address.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> The XML file creates two columns for each monitor reading; one containing the value with units, and the other containing just the value. This is to make it easier to import the XML data into a third party application which may not automatically separate data values from the text describing the units.</p>
<b>Send XML file by email</b>	If you enter an email address in the text box, SiteScope sends a copy of the XML file to that address.

## Calculation Method

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Best case calculation</b>	Select this option to calculate the monitor uptime percentage, warning percentage, and error percentage using a best case scenario. In this scenario, monitor time in error is calculated from the first monitor run that explicitly reported an Error instead of from the time of the last known Good monitor run.
<b>Time between samples</b>	Use this time scale option to choose the time interval between monitor readings. You can choose intervals that range from once every minute to once a day, or you can use the automatic scaling. When automatic scaling is used, SiteScope determines how many readings were taken over the chosen time period for the given monitors and then selects an appropriate interval for the management report. <b>Default value:</b> Automatic time scale
<b>Maximum graph value</b>	Select a vertical scale option to choose the maximum value displayed on a graph. Choosing a specific scale value makes it easier to compare graphs from different monitors and times. <b>Default value:</b> Automatic vertical scale

## Management Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Disable</b>	Select to temporarily disable the generation of this report. To enable the report again, clear the box. <b>Default value:</b> Not selected
<b>Generate report at (HH:MM)</b>	The time that you want SiteScope to create this management report. The report contains information for the last day, week, or month, ending at the time the report is run. For example, if a daily report is generated at 18:00 (6:00 p.m.), it contains data generated between 18:00 the previous day and 18:00 of the current day. The default value is 00:00 which represents midnight. <b>Default value:</b> 04:00 <b>Note:</b> SiteScope Management report generation may temporarily affect overall SiteScope performance and responsiveness depending on the number of monitors and time period of the report. Try to schedule reports to be generated during off-peak hours relative to overall monitoring tasks and load. If you are generating many reports each day, you should consider staggering the <b>Generate report at</b> value for different reports.



## Search/Filter Tags

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Tag name and values>	<p>Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.</p> <p>For details on using tags, see “Working with Search/Filter Tags” on page 107.</p>
<b>Add Tag</b>	<p>Click to add a new keyword tag.</p> <p>For details on the New SiteScope Tag user interface, see “New/Edit Tag Dialog Box” on page 116.</p>

---

**Note:** A bar graph is generated using standard HTML, so it can be printed from all browser types. Line graphs are generated using a java applet and may not print directly from all browsers.

---

## Graph Measurement Options

This table includes a description of the graph measurement options that can be included in the report:

Graph	Description
<b>None - no graph</b>	No graphs are included in the report. The report only includes the tabular data contents you have selected.
<b>Bar graph - one graph per measurement</b>	This bar graph option displays a single type of measurement per graph and per monitor during the specified time frame. For reports on multiple monitors, this results in the most number of graphs with one bar graph generated for each type of measurement for each monitor.
<b>Line Graph - one graph per measurement</b>	This line graph option displays a separate line graph for each type of measurement for a single monitor. Like the bar graph option, this results in the most number of line graphs with one line graph generated for each type of measurement for each monitor selected for the report regardless of any compatibility of measurement type.
<b>Line Graph - group per monitor instance</b>	This line graph option attempts to group all measurements from a single monitor instance into a single graph per monitor. The number of line graphs actually generated depends on whether the monitor records multiple measurements per monitor run (for example, the Microsoft Windows Resources or UNIX Resources monitor types) and whether the measurement types are compatibility with one another. Separate graphs are generated if the measurement types are not compatible.


Graph	Description
<b>Line Graph - group same measurement types</b>	Select this option to plot the same measurement types gathered by several different monitor instances into single graphs. A line graph is generated for each set of compatible measurement types regardless of the number of monitors selected for the report.
<b>Line Graph - group compatible measurements</b>	Select this option to display all compatible measurements from the selected monitors on a single graph. The option is intended to minimize the total number of line graphs generated. The number of graphs generated is still dependent on the compatibility of the selected monitor types and the measurement types collected by those monitors. If all of the monitors selected for the report are of the same type, for example URL monitors, then a single graph is generated with a colored line for each of the monitors.

---

**Note:** A bar graph is generated using standard HTML, so it can be printed from all browser types. Line graphs are generated using a java applet and may not print directly from all browsers.

---

## New SiteScope Quick Report Dialog Box

<b>Description</b>	<p>Enables you to create a one-time SiteScope management report for any monitor or group of monitors over a given time period.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor, and select <b>Reports &gt; Quick</b>. Alternatively, select a monitor and click the <b>Report</b>  button in Dashboard.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The time interval for a Quick report is not incremented automatically. This means that a Quick report always contain the data for the absolute <b>Report period</b> interval defined in the report definition. To view more recent data using a Quick report, edit the <b>Report period</b> setting.</li> <li>▶ When working in Business Availability Center, Quick Report definitions in System Availability Management Administration are stored only with the Business Availability Center context. Quick Report definitions are not stored in, and do not persist on the SiteScope server.</li> </ul>
<b>Included in Tasks</b>	“Create a Report” on page 2041
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Reports Overview” on page 2035</li> <li>▶ “Quick Report” on page 2076</li> </ul>

### Report Targets

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Report targets</b>	<p>Select the groups and/or monitors to be included in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers.</p> <p><b>Default value:</b> The current container and all child elements are selected.</p>

## Display Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Thresholds</b>	
<b>All thresholds</b>	Creates a table of monitor error, warning, and good threshold settings for all of the monitors included in the report. If selected, this table is displayed as the first report section. <b>Default value:</b> Not selected
<b>Error thresholds</b>	Creates a table of individual error readings recorded by the monitors during the report period. <b>Default value:</b> Selected
<b>Warning thresholds</b>	Creates a table of individual warning readings recorded by the monitors during the report period. <b>Default value:</b> Selected
<b>Good thresholds</b>	Creates a table of individual good readings recorded by the monitors during the report period. <b>Default value:</b> Selected
<b>Uptime and Readings</b>	
<b>Uptime Summary and Measurement Summary tables</b>	Creates two report tables: <b>Uptime Summary</b> and <b>Measurement Summary</b> . For details of the data included in these tables, see “Report Content” on page 2078. <b>Default value:</b> Selected
<b>Uptime: Include warnings</b>	Includes any monitor readings that are reported as warnings in the overall Uptime calculation. <b>Default value:</b> Not selected

GUI Element	Description
<b>Uptime: Ignore warning</b>	<p>Suppresses monitor readings reported as warnings from the overall Uptime and Readings Summary section.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> This option only suppresses the display of the Warning % column in the table; it does not change the calculation of the Uptime %.</p>
<b>Uptime: Ignore errors</b>	<p>Suppresses monitor readings reported as errors from the overall Uptime and Readings Summary section.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> This option only suppresses the display of the Error % column in the table; it does not change the calculation of the Uptime %.</p>
<b>General Settings</b>	
<b>Measurements graph</b>	<p>For graph reports, use the drop-down list to choose a graphical measurement to be included in the report. For details of the options, see "Graph Measurement Options" on page 2058.</p> <p><b>Default value:</b> Bar Graph - one graph per measurement</p>
<b>Monitor readings</b>	<p>Creates a table of individual readings recorded by the monitors during the report period, including all readings (error, good, and warning). This report table may also include blank "buckets" depending on the period of the report and how often the monitors ran during the period.</p> <p><b>Default value:</b> Selected</p>

GUI Element	Description
<b>Alerts table</b>	<p>Select an option to include a table of alerts sent for the monitors in the report. The options for the alerts table level are:</p> <ul style="list-style-type: none"> <li>▶ <b>No alerts table.</b> No table of alerts is included in the report (default).</li> <li>▶ <b>Basic alerts table.</b> Displays the time and summary information for each alert sent.</li> <li>▶ <b>Show detailed alerts table for all alerts.</b> Displays detailed alert information for each alert in the report.</li> <li>▶ <b>Show detailed alerts table for failed alerts.</b> Displays the time and summary information for each alert, and a full diagnostics breakdown for each failed alert.</li> </ul>
<b>Detailed monitor information</b>	<p>Displays all of the information gathered for each monitor on the report. Otherwise, only the primary data is displayed for each monitor.</p> <p><b>Example:</b> If this box is checked on a URL Sequence Monitor, the timing information for each step in the sequence is displayed in the report.</p> <p><b>Default value:</b> Not selected</p>
<b>Time in error</b>	<p>Creates a table summary listing each monitor selected for the report with a summary of how many minutes the monitor status was calculated as being in error for the period of the report.</p> <p><b>Default value:</b> Not selected</p>

## Filter and Scheduling Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Monitor filter</b>	<p>Select a subset of those monitors to be shown in the report—those that have had the specified status sometime during the report's time frame. You can select only monitors in Error or Warning, monitors in Error, monitors in Warning, monitors that were OK, or all monitors.</p> <p><b>Default value:</b> Show all monitors</p> <p><b>Example:</b> Choosing <b>Show only monitors in error</b> displays report data only if that monitor had spent time in error sometime during the time interval of the report.</p>
<b>Schedule filter</b>	<p>Select a schedule filter option for showing only a subset of the data in the report—those monitors that have samples during the time period of the schedule.</p> <p><b>Default value:</b> The report shows data for the full period of the report (every day, all day).</p> <p><b>Example:</b> Choosing <b>weekdays, 09:00-18:00</b> displays report data for the selected monitors with samples from the 9am to 6pm time period, Monday through Friday. Only this data is used for all the calculations.</p>
<b>Report period</b>	<p>Specify the time period for which you want to view monitoring data. Enter the time from which you want the report coverage to start in the <b>From</b> boxes and the time to which you want to cover in the <b>To</b> boxes.</p> <p><b>Default value:</b> The time period is from one hour before the time that the Quick Report is generated until the current time. You can set the default time period for including monitoring data in the Quick report by configuring the <b>Quick report time period (hours)</b> setting in <b>Preferences &gt; Infrastructure Preferences &gt; Reports</b>.</p> <p><b>Note:</b> Times should be entered in 24-hour format.</p>



## Report Format

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Report in</b>	Select the format to be used in displaying the report: HTML format, Text format or XML format. <b>Default value:</b> HTML format
<b>File format</b>	This option enables some customization of the report appearance. The options are: <ul style="list-style-type: none"> <li>➤ <b>Color background</b> (default)</li> <li>➤ <b>Color background, no table borders</b></li> <li>➤ <b>White background</b></li> </ul>

## Report Distribution

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Send report to email address</b>	To have the report forwarded by email when it is generated, enter the email address(es) to which this report should be sent each time its generated. To send the reports to multiple email addresses, separate the email addresses with commas.

## Calculation Method

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Best case calculation</b>	<p>Select this option to calculate the monitor uptime percentage, warning percentage, and error percentage using a best case scenario. In this scenario, monitor time in error is calculated from the first monitor run that explicitly reported an Error instead of from the time of the last known Good monitor run.</p> <p><b>Default value:</b> Not selected</p>
<b>Time between samples</b>	<p>Use this time scale option to choose the time interval between monitor readings. You can choose intervals that range from once every minute to once a day, or you can use the automatic scaling. When automatic scaling is used, SiteScope determines how many readings were taken over the chosen time period for the given monitors and then selects an appropriate interval for the management report.</p> <p><b>Default value:</b> Automatic time scale</p>
<b>Maximum graph value</b>	<p>Select a vertical scale option to choose the maximum value displayed on a graph. Choosing a specific scale value makes it easier to compare graphs from different monitors and times.</p> <p><b>Default value:</b> Automatic vertical scale</p>

## New SiteScope Monitor Report Dialog Box

<b>Description</b>	Enables you to create a report that provides detailed information about the monitors defined in one or more monitor groups.  <b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor, and select <b>Reports &gt; Monitor</b> .
<b>Included in Tasks</b>	“Create a Report” on page 2041
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “SiteScope Reports Overview” on page 2035</li> <li>➤ “Monitor Summary Report” on page 2080</li> </ul>

### Report Targets

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Report targets</b>	Select the groups and/or monitors to be included in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers.  <b>Default value:</b> The current container and all child elements are selected.

## Display Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Display columns</b>	<p>Select the monitor information to display in the report columns. Data is shown in the report for the selected parameters only if the particular option has been selected, such as Disabled and Frequency, or if a value has been supplied, such as Monitor Description. If the option or value has not been defined in the particular monitor setup, the column is blank for that parameter for that monitor.</p> <p><b>Note:</b> Hold down the SHIFT key to select a set of adjacent groups. Use CTRL-click to select non-adjacent items.</p>
<b>Show parameters</b>	<p>Select if you want the report to contain the parameters defined for each monitor. This option includes a list of the active options defined for each selected monitor in a single table cell rather than individual columns as with the option above.</p> <p><b>Default value:</b> Selected</p>
<b>Sort by</b>	<p>Select the monitor parameter to use as a sort key for the report.</p> <p><b>Default value:</b> Monitor Type</p>
<b>Sort order</b>	<p>Select the order to use for sorting the report. For example, to sort the report alphabetically by monitor type, select Monitor Type, and select Ascending sort order.</p> <p><b>Default value:</b> Ascending</p>

## Export Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<b>Export to file</b>	Select this box to have SiteScope export the Monitor Summary report data to a text file. <b>Default value:</b> Not selected
<b>File name</b>	When the <b>Export to file</b> option is enabled, SiteScope writes the data to the file name specified here using the selected text format. The file is written into the <b>&lt;SiteScope root directory&gt;\htdocs</b> directory. <b>Default value:</b> monSummary
<b>File format</b>	Select the format for the exported file. The options are comma-delimited text, tab delimited text, or HTML. <b>Default value:</b> comma-delimited (csv)

## New SiteScope Alert Report Dialog Box

<b>Description</b>	Enables you to create a report used to display SiteScope alerts sent over a given time period.  <b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor, and select <b>Reports &gt; Alert</b> .
<b>Included in Tasks</b>	“Create a Report” on page 2041
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “SiteScope Reports Overview” on page 2035</li> <li>▶ “Alert Report” on page 2083</li> </ul>

### Report Targets

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Report targets</b>	Displays the groups and/or monitors to be included in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers.  <b>Note:</b> You cannot remove any of the groups or monitors in the selected container from the report.

## Alert Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Alert types</b>	<p>Select the alert types that you want to include in the report.</p> <p><b>Note:</b> Hold down the <code>SHIFT</code> key to select a set of adjacent groups. Use <code>CTRL</code>-click to select non-adjacent items.</p>
<b>Detail level</b>	<p>Select the level of detail to include in the report. The options are:</p> <ul style="list-style-type: none"> <li>▶ <b>Basic.</b> Displays the time and summary information for each alert sent (default setting).</li> <li>▶ <b>Detail for all alerts.</b> Displays detailed alert information for each alert in the report.</li> <li>▶ <b>Detail for failed alerts.</b> Displays the time and summary information for each alert, and a full diagnostics breakdown for each failed alert.</li> </ul>
<b>Alert time period</b>	<p>Specify the period of time that you want the report to cover. Select or enter the time and date you want report coverage to start in the <b>From</b> boxes and the time and date you want coverage to end in the <b>To</b> boxes.</p> <p><b>Default value:</b> The alert time period is from one hour before the time that the Alert Report is generated until the current time.</p> <p><b>Note:</b> Times must be entered in 24-hour format.</p>

## Management Report

The following is an example of the Management report.

Management SiteScope Report "Cor...ort"
Properties **View Report**

[Table Format](#)  
[Error List](#)  
[Warning List](#)  
[Good List](#)

[Index of Reports](#)

### Core Weekly Report

(information from 9:34 AM 12/3/07 to 9:34 AM 12/4/07 )


#### Uptime Summary

Name	Uptime %	Error %	Warning %	Last
CPU Utilization on SiteScope Server	100	0	0	good
Memory on SiteScope Server	100	0	0	good
FTP on localhost	100	0	0	good
URL List	0	0	0	good
Disk Space: C on SiteScope Server	100	0	0	good
Directory: c:\ on SiteScope Server	100	0	0	good
Service: HTTP on SiteScope Server	100	0	0	good

#### Measurement Summary

Name	Measurement	Max	Avg	Last
<a href="#">CPU Utilization on SiteScope Server</a>	utilization	74%	28.08%	24%
<a href="#">Memory on SiteScope Server</a>	percent used	22%	22%	22%
<a href="#">FTP on localhost</a>	round trip time	0.02 sec	0.01 sec	0.016 sec
<a href="#">URL List</a>	errors	0 URLs	0 URLs	0 URLs
<a href="#">Disk Space: C on SiteScope Server</a>	percent full	32%	32%	32%
<a href="#">Directory: c:\ on SiteScope Server</a>	total of file sizes	10998795264 bytes	10997342208 bytes	10998795264 bytes



<b>Description</b>	<p>Displays a summary and specific details of infrastructure availability and performance data for monitors and monitor groups over a given period of time. Use Management reports to detect emerging trends and correct potential problems before they become a crisis.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor container, and select <b>Reports &gt; Management</b>. Configure the report properties, and click <b>OK</b>. In the Reports tab, select the report and click the <b>Generate Report</b>  button. Click the date-coded link for the report period you want to view. If no reports have been generated, or if you want to create an updated report, click the <b>Generate</b> button.</p>
<b>Included in Tasks</b>	“Create a Report” on page 2041
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>➤ “Working with SiteScope Management Reports” on page 2039</li> <li>➤ “New/Edit SiteScope Management Report Dialog Box” on page 2045</li> <li>➤ “Reports Page” on page 2043</li> </ul>

## Report Content - Index Page

The following elements are included in the Management report index page:

GUI Element	Description
<b>Most Recent Report</b>	Click to display the most recent Management report available for the currently selected monitor or group.
<b>Information For &lt;report time and data&gt;</b>	Click to display the Management report for the time period specified in the link for the currently selected monitor or group. For details on the Management Report page, see “Report Content - Management Report Page” below.
<b>Generate</b>	Click to create a new report for the currently selected monitor or group, regardless of when the report was normally scheduled to be generated.

## Report Content - Management Report Page

The following elements are included in the Management report page:

GUI Element	Description
<b>Table Format</b>	Click the <b>Table Format</b> link to go to the measurements data in table format in the currently selected report.
<b>Error List</b>	Click the <b>Error List</b> link to go to the list of monitors with error status in the currently selected report.
<b>Warning List</b>	Click the <b>Warning List</b> link to go to the list of monitors with warning status in the currently selected report.
<b>Good List</b>	Click the <b>Good List</b> link to go to the list of monitors with good status in the currently selected report.
<b>Index of Reports</b>	Click the <b>Index of Reports</b> link to go to the index of Management reports. For details on the Management Report index page, see “Report Content - Index Page” on page 2073.
<b>Uptime Summary</b>	<p>This table includes the following:</p> <ul style="list-style-type: none"> <li>▶ <b>Name.</b> The name of monitors included in the report.</li> <li>▶ <b>Uptime %.</b> The percentage of monitor readings reported as good.</li> <li>▶ <b>Warning %.</b> The percentage of monitor readings reported as warning.</li> <li>▶ <b>Error %.</b> The percentage of monitor readings reported as error.</li> <li>▶ <b>Last.</b> The last reading of the monitor for the report period.</li> </ul>

GUI Element	Description
<b>Measurement Summary</b>	This table includes the following: <ul style="list-style-type: none"> <li>➤ <b>Name.</b> The name of monitors included in the report.</li> <li>➤ <b>Measurement.</b> The parameter being monitored (for error condition).</li> <li>➤ <b>Max.</b> The maximum value recorded for the Measurement parameter during the report period.</li> <li>➤ <b>Avg.</b> The average value of the readings recorded for the report period.</li> <li>➤ <b>Last.</b> The last reading of the monitor for the report period.</li> </ul>
<Measurement Graphs>	Measurement data in graph format for each monitored instance for the report period.
<Measurement Tables>	Measurement data in table format, shown at 30 minute increments, for each monitored instance for the report period. Entries highlighted in red or yellow indicate that the measurement exceeded the error or warning status threshold for the monitor. Blue indicates that the monitor was disabled.
<Error List Table>	Lists the monitor instances that exceeded the error status threshold for the monitor. Entries are highlighted in red.
<Warning List Table>	Lists the monitor instances that exceeded the warning status threshold for the monitor. Entries are highlighted in yellow.
<Good List Table>	Lists the monitor instances that were in the good status threshold for the monitor. Entries are highlighted in green.

## Quick Report

The following is an example of the Quick report.

**Evaluation license for 1,000 points, 9 days remaining**

---

[Table Format](#)

[Error List](#)

[Warning List](#)

[Good List](#)

[Close Window](#)

### Summary for Multiple Monitors


(information from 7:53 AM 11/1/07 to 8:53 AM 11/1/07 )

#### Uptime Summary

Name	Uptime %	Error %	Warning %	Last
Log Event Checker	100	0	0	good
Monitor Load Checker	100	0	0	good
BAC Integration Statistics	100	0	0	good
Health of SiteScope Server	100	0	0	good
cpu on core	0	0	0	DISABLED
memory on core	0	0	0	DISABLED
ping	0	100	0	ERROR

#### Measurement Summary

Name	Measurement	Max	Avg	Last
<a href="#">Log Event Checker</a>	Currently logging to Business Availability Center	0	0	0
<a href="#">Log Event Checker</a>	Current Monitors Running	0	0	0
<a href="#">Log Event Checker</a>	Current Monitors Waiting	0	0	0

<b>Description</b>	<p>Displays a summary and specific details of infrastructure availability and performance data for monitors and monitor groups over a given period of time. Quick reports are generated on an ad hoc basis and are not saved to the SiteScope configuration data.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor container, and select <b>Reports &gt; Quick</b>. Alternatively, select a monitor and click the <b>Report</b>  button in Dashboard. Configure the report properties, and click <b>Generate Report</b>.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The time interval for a Quick report is not incremented automatically. This means that the report always contains the data for the absolute <b>Report Period</b> interval defined in the report definition. To view more recent data using a Quick report, edit the <b>Report Period</b> setting.</li> <li>▶ When working in Business Availability Center, Quick Report definitions in System Availability Management Administration are stored only with the Business Availability Center context. Quick Report definitions are not stored in and do not persist on the SiteScope server.</li> </ul>
<b>Included in Tasks</b>	“Create a Report” on page 2041
<b>Useful Links</b>	“New SiteScope Quick Report Dialog Box” on page 2060

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<License details>	License details are displayed at the top of the page. It includes the SiteScope license category, the number of monitor points available, and the number of days remaining on the license.
<b>Table Format</b>	Click to go to the measurements data in table format in the currently selected report.
<b>Error List</b>	Click to go to the list of monitors with error status in the currently selected report.
<b>Warning List</b>	Click to go to the list of monitors with warning status in the currently selected report.
<b>Good List</b>	Click to go to the list of monitors with good status in the currently selected report.
<b>Uptime Summary</b>	<p>This table includes the following:</p> <ul style="list-style-type: none"> <li>▶ <b>Name.</b> The name of monitors included in the report.</li> <li>▶ <b>Uptime %.</b> The percentage of monitor readings reported as good.</li> <li>▶ <b>Warning %.</b> The percentage of monitor readings reported as warning.</li> <li>▶ <b>Error %.</b> The percentage of monitor readings reported as error.</li> <li>▶ <b>Last.</b> The last reading of the monitor for the report period.</li> </ul>

GUI Element	Description
<p><b>Measurement Summary</b></p>	<p>This table includes the following:</p> <ul style="list-style-type: none"> <li>➤ <b>Name.</b> The name of monitors included in the report.</li> <li>➤ <b>Measurement.</b> The parameter being monitored (for error condition).</li> <li>➤ <b>Max.</b> The maximum value recorded for the Measurement parameter during the report period.</li> <li>➤ <b>Avg.</b> The average value of the readings recorded for the report period.</li> <li>➤ <b>Last.</b> The last reading of the monitor for the report period.</li> </ul>
<p>&lt;Measurement Graphs&gt;</p>	<p>Measurement data in graph format for each monitored instance for the period of the report.</p>
<p>&lt;Measurement Tables&gt;</p>	<p>Measurement data in table format, shown at 30 minute increments, for each monitored instance for the period of the report. Entries highlighted in red or yellow indicate that the measurement exceeded the error or warning status threshold for the monitor. Blue indicates that the monitor was disabled.</p>
<p>&lt;Error List Table&gt;</p>	<p>Lists the monitor instances that exceeded the error status threshold for the monitor. Entries are highlighted in red.</p>
<p>&lt;Warning List Table&gt;</p>	<p>Lists the monitor instances that exceeded the warning status threshold for the monitor. Entries are highlighted in yellow.</p>
<p>&lt;Good List Table&gt;</p>	<p>Lists the monitor instances that were in the good status threshold for the monitor. Entries are highlighted in green.</p>

 **Monitor Summary Report**

The following is an example of the Monitor Summary report.

SiteScope Monitor Summary Report					
Group	name	class	frequency	disabled	schedule
AutoSanity: Basic	URL List	URL List	1 hour		
AutoSanity: Basic	Service: HTTP on SiteScope Server	Service	10 minutes		
AutoSanity: Basic	FTP on localhost	Port	1 minute		
Health	Monitor Load Checker	Monitor Load Monitor	100 seconds		
AutoSanity: Basic	Memory on SiteScope Server	Memory	1 minute		
Health	Log Event Checker	Log Event Health Monitor	10 minutes		
AutoSanity: Basic	Link Check: http://www.google.com	Link Check	1 hour		
Health	Health of SiteScope Server	Health of SiteScope Server	5 minutes		
EMS	EMS Log File on SiteScope Server	EMS Log File	10 minutes		
AutoSanity: Basic	Disk Space: C on SiteScope Server	Disk Space	1 minute		
AutoSanity: Basic	Directory: c:\ on SiteScope Server	Directory	1 minute		
AutoSanity: Basic: DisabledGroup	disabledMonitor	CPU Utilization	10 minutes	disabled	
AutoSanity: Basic	CPU Utilization on SiteScope Server	CPU Utilization	1 minute		
Health	BAC Integration Statistics	BAC Integration Statistics	100 seconds		

[Close Window](#)



<b>Description</b>	<p>Displays information about the configuration and current settings of monitors in the groups you have selected to include in the report.</p> <p>Use this report to view setup information on monitors as well as the organization and makeup of groups of monitors. For example, you can check and compare monitor run frequencies (the <b>Frequency</b> setting) if you are having problems with monitor skips. You can also use the report to check for monitor dependencies that can impact alerting.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor container, and select <b>Reports &gt; Monitor</b>. Configure the report properties, and click <b>Generate Report</b>.</p>
<b>Included in Tasks</b>	“Create a Report” on page 2041
<b>Useful Links</b>	“New SiteScope Monitor Report Dialog Box” on page 2067

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element	Description
<b>Group</b>	The group name to which the monitor belongs.
<b>Name</b>	The display name or text description for each monitor.
<b>Class</b>	The monitor type.
<b>Frequency</b>	The frequency at which the monitor is set to run.
<b>Disabled</b>	Whether or not the monitor is disabled.
<b>Depends on</b>	Lists any dependent monitors, if the running of this monitor is dependent on the status of other monitors.

GUI Element	Description
<b>Points</b>	The number of license points used by the monitor instance.
<b>OID</b>	The Object ID for this monitor.
<b>Schedule</b>	The monitor schedule, if a schedule other than the default schedule is selected.
<b>Error Frequency</b>	If the <b>Error frequency</b> option is selected, the monitoring interval, in seconds, for monitors that have reported an error condition.
<b>Timeout</b>	The timeout setting for the monitor.
<b>Verify Error</b>	Displays On if the <b>Verify error</b> option is selected. This option automatically runs the monitor again if it detects an error.
<b>Monitor Description</b>	The text description for the monitor in the Monitor Description box.
<b>Thresholds</b>	The threshold conditions for the monitor instance.

# Alert Report

The following is an example of the Alert report.

**Alerts (SiteScope) from 4:20 PM 7/30/07 to 4:26 PM 7/30/07**

Time	Type	Message	Monitor	Group
4:20 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:21 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:22 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:23 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:24 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:25 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:26 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36



<b>Description</b>	<p>Displays information about SiteScope alerts generated during a specified period of time for the monitors in the selected container.</p> <p><b>To access:</b> Open the <b>Monitors</b> context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor container, and select <b>Reports &gt; Alert</b>. Configure the report properties, and click <b>Generate Report</b>.</p>
<b>Included in Tasks</b>	“Create a Report” on page 2041
<b>Useful Links</b>	“New SiteScope Alert Report Dialog Box” on page 2070

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):



GUI Element	Description
<Report title>	The report title contains the name of the monitor group container or individual monitor for which the report was created, and the time period that the report covers.
<b>Time</b>	The time at which the alert was triggered.
<b>Type</b>	The type of alert action.
<b>Message</b>	The type of message in the alert (for example, Default, alarm).
<b>Monitor</b>	The name of the monitor on which the alert was triggered.
<b>Group</b>	The name of the group on which the alert was triggered.








## Annotation Tool



<b>Description</b>	<p>Enables you to annotate a snapshot of the report you are viewing, to highlight important areas. The Annotation Tool is available when viewing Baseline Monitor Measurements Graphs and Server-Centric reports.</p> <p>The Annotation Options enable you to customize your snapshot. The Annotation Menu Bar contains elements that enable you to:</p> <ul style="list-style-type: none"> <li>▶ Change the appearance of the snapshot.</li> <li>▶ Save, print, or email an annotation report.</li> <li>▶ Customize the appearance of text annotated onto your snapshot. These elements are enabled only when the Text Tool button  is selected.</li> </ul> <p><b>To access:</b> Click the <b>Annotate</b> button  on the right side of the page.</p>
<b>Important Information</b>	<p>To use the Annotation Tool, the Sun JRE plug-in 1.6.0_x (latest version recommended) must be installed on your machine. If the plug-in is not installed on your machine, you are prompted to install it.</p>
<b>Useful Links</b>	<ul style="list-style-type: none"> <li>▶ “Generating a Server-Centric Report” on page 1881</li> <li>▶ “Server-Centric Report” on page 1890</li> <li>▶ “Setting Status Thresholds Using a Baseline” on page 312</li> </ul>

### Annotation Options

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Click to navigate the snapshot.
	Click to select a specific area of the snapshot.

GUI Element (A–Z)	Description
	<p>Click to add a shape to the snapshot. Clicking the shape tool button enables the following shape buttons:</p> <ul style="list-style-type: none"> <li>▶  Click to mark an area of the snapshot with a rectangle.</li> <li>▶  Click to mark an area of the snapshot with a filled rectangle.</li> <li>▶  Click to mark an area of the snapshot with an oval.</li> <li>▶  Click to mark an area of the snapshot with a filled oval.</li> <li>▶  Click to mark an area of the snapshot with a round rectangle.</li> <li>▶  Click to mark an area of the snapshot with a filled round rectangle.</li> </ul> <p><b>Customization.</b> After selecting this button, you can customize your line appearance through the following parts of the interface:</p> <ul style="list-style-type: none"> <li>▶ <b>Line Type.</b> Choose the type of line you want to add. Options include: <ul style="list-style-type: none"> <li>▶ Solid Line</li> <li>▶ Jagged Line</li> </ul> </li> <li>▶ <b>Line Width.</b> Select the width of the line, in pixels, in the annotation.</li> </ul>













GUI Element (A–Z)	Description
	<p>Click to enable the line tool, which marks the selected area of the snapshot with a line.</p> <p><b>Customization.</b> After selecting this button, you can customize your line appearance through the following parts of the interface:</p> <ul style="list-style-type: none"> <li>▶ <b>Line Style.</b> Choose the style of line you want to add. Options include: <ul style="list-style-type: none"> <li>▶ Regular line</li> <li>▶ Line with endpoints</li> <li>▶ Line with arrows</li> </ul> </li> <li>▶ <b>Line Type.</b> Choose the type of line you want to add. Options include: <ul style="list-style-type: none"> <li>▶ Solid Line</li> <li>▶ Jagged Line</li> </ul> </li> <li>▶ <b>Line Width.</b> Select the width of the line, in pixels, in the annotation.</li> </ul>
	<p>Click to add text to the snapshot.</p> <p><b>Example:</b> Add the syntax This is the problematic transaction above a line marking an area of the report.</p>










GUI Element (A-Z)	Description
<b>Border and Fill Colors</b>	<p>Select the relevant square to choose the color of the border and fill of your annotations. The available squares are:</p> <ul style="list-style-type: none"> <li>➤ <b>Upper Square.</b> Click to choose the color of lines, as generated by the line tool and displayed in unfilled shapes.</li> <li>➤ <b>Lower Square.</b> Click to choose the color to fill shapes. Clicking either of the squares generates a dialog box with the following tabs where you choose the color: <ul style="list-style-type: none"> <li>➤ Swatches</li> <li>➤ HSB</li> <li>➤ RGB</li> </ul> </li> </ul>
<b>Opacity</b>	<p>Slide the opacity bar to choose the darkness level of the selected shape line, text line, or shape color in the annotation.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>➤ A higher opacity percentage means that the selection appears darker. A lower opacity percentage means that the selection appears lighter.</li> <li>➤ This field is enabled when either the shape tool, line tool, or text tool button is selected.</li> </ul>



## Annotation Menu Bar

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A–Z)	Description
	Click to save the snapshot on your local machine. <b>Note:</b> <ul style="list-style-type: none"> <li>▶ The snapshot is saved in .png format.</li> <li>▶ You cannot select the <b>New Folder</b> icon  when saving in the <b>My Documents</b> directory or any of its subdirectories.</li> </ul>
	Click to select all of the annotations added to your snapshot.
	Click to clear all annotations.
	Click to undo the most recent action performed on the snapshot.
	Click to redo the most recent action performed on the snapshot.
	Click to bring the snapshot view closer.
	Click to set the snapshot view further away.
	Click to restore the snapshot to its original size.
	Click to print the snapshot.
	Click to send the snapshot via email.
	Click to display online documentation help for the page you are currently viewing.

GUI Element (A-Z)	Description
	<p>Click to mark the text as bold.</p> <p><b>Note:</b> This field is enabled only when selecting the <b>Text Tool</b> button .</p>
	<p>Click to mark the text as italicized.</p> <p><b>Note:</b> This field is enabled only when selecting the <b>Text Tool</b> button .</p>
	<p>Click to mark the text as underlined.</p> <p><b>Note:</b> This field is enabled only when selecting the <b>Text Tool</b> button .</p>
<Font Family>	<p>Select the font for the text in the report.</p> <p><b>Note:</b> This field is only enabled when selecting the <b>Text Tool</b> button .</p>
<Font Size>	<p>Select the size of the font in the report.</p> <p><b>Note:</b> This field is only enabled when selecting the <b>Text Tool</b> button .</p>
<b>Anti-aliasing</b>	<p>Select to adjust the pixel reading of text or annotation lines so that they appear smoother.</p> <p><b>Note:</b> This field is only enabled when selecting the <b>Text Tool</b> button .</p>

---

## System Availability Management Reports

This chapter describes System Availability Management reports which are based on data collected by the SiteScope data collector.

---

**Note:** The System Availability Management reports are available only to HP Business Availability Center users.

---

### **This chapter includes:**

#### **Concepts**

- ▶ System Availability Management Reports Overview on page 2092
- ▶ Working with System Availability Management Reports on page 2093
- ▶ SiteScope Over Time Reports on page 2095
- ▶ Understanding the Cross-Performance Report Scale on page 2098
- ▶ Understanding the Group Performance Report on page 2099
- ▶ System Availability Management Data in Custom Reports on page 2100

#### **Tasks**

- ▶ Create a Monitor Performance Report – Workflow on page 2102
- ▶ Create a Cross-Performance Report – Workflow on page 2103
- ▶ Rescale a Cross-Performance Report on page 2104

#### **Reference**

- ▶ System Availability Management Reports User Interface on page 2104

## System Availability Management Reports Overview

You use the System Availability Management application to view and analyze reports based on the performance data collected by the SiteScope data collector and stored in the HP Business Availability Center database.

In addition, using SiteScope Infrastructure Monitors, you can integrate data collected by enterprise management systems (such as BMC Patrol, Tivoli, Concord, and NetIQ) into HP Business Availability Center, and view the data in System Availability Management reports.

System Availability Management utilizes data collected by SiteScope and enables you to:

- ▶ monitor system availability across the entire enterprise infrastructure from a centralized, real-time perspective
- ▶ apply a business perspective to system management view data at the application level rather than viewing numerous low-level system metrics
- ▶ view information about events collected from external applications or software and SiteScope events

---

**Note:**

- ▶ You access the System Availability Management reports from the System Availability Management application in the Applications menu.
- ▶ For details on working with HP Business Availability Center reports, see “Working in Reports” in *Reports* in the HP Business Availability Center Documentation Library.

---

This section includes the following topics:

- ▶ “Report Access and Permissions” on page 2093
- ▶ “Data Aggregation” on page 2093

## Report Access and Permissions

The availability of report data to a specific user is dependent on the profile access permissions granted to that user. Furthermore, access to specific data within a profile may also be filtered by using the group permission filters. For details on granting permissions, see “Permissions Overview” in *Platform Administration* in the HP Business Availability Center Documentation Library. For details on defining group permission filters, see “System Availability Management Administration (SAM Admin)” in *Platform Administration* in the HP Business Availability Center Documentation Library.

## Data Aggregation

HP Business Availability Center uses data aggregation to make data handling and management more efficient and to improve the speed and performance of report generation. For information about data aggregation in HP Business Availability Center, see “Data Aggregation” in *Reference Information* in the HP Business Availability Center Documentation Library.

## Working with System Availability Management Reports

System Availability Management reports help you identify server resource usage trends, as well as bottlenecks and other server-related issues that may be contributing to application performance problems. You can continually monitor report data to identify poor server performance or to spot developing trends that may lead to server performance problems.

Alternatively, when you become aware of a performance problem with your application (for example, after analyzing End User Management reports or receiving an alert), you can use System Availability Management reports to help you identify, or rule out, infrastructure machine-related issues as the root cause of the problem. By analyzing the infrastructure machine resource usage data for the same time period during which the performance problem occurred, you can assess whether one or more infrastructure machine resource measurements are outside normal performance thresholds for that time period.

## Improving Report Generation Times

---

**Note to HP Software-as-a-Service customers:** This section is not relevant for HP Software-as-a-Service customers.

---

To optimize the performance of System Availability Management report generation, we recommend that a database administrator perform an update statistics procedure to the database on a regular basis. The regularity of the update depends on the amount of data generated by the applications you are monitoring.

► **Microsoft SQL Server users.**

- for a small site, you should update once every three to four days
- for a medium site, you should update daily
- for a large site, you should update every four hours

For details on Microsoft SQL Server maintenance, see “Maintenance Plan” in the *HP Business Availability Center Database Guide* PDF.

► **Oracle Server users.** Analyze all tables according to database size.

For details on optimizing performance in Oracle, see “Collecting Statistics for Databases” in the *HP Business Availability Center Database Guide* PDF.

## SiteScope Over Time Reports

The SiteScope Over Time reports are the individual reports displayed in the System Availability Management application in HP Business Availability Center. You use the SiteScope Over Time reports to view and analyze infrastructure machine-related data collected by the SiteScope data collector and stored in the HP Business Availability Center database. You cross-reference this data with transaction performance problems, such as slow transaction response times and failed transactions, to understand the root cause of application performance issues.

The contents of SiteScope Over Time reports depend on the types of SiteScope monitors and measurements that are defined in System Availability Management Administration.

HP Business Availability Center users can use group permissions filters to control the data that System Availability Management reports display. This enables filtering data that may be irrelevant to a specific user, making reports more manageable and report generation faster. For details, see “System Availability Management Administration (SAM Admin)” in *Platform Administration* in the HP Business Availability Center Documentation Library.

**Note:**

- For details on generating reports, see “Working in Reports” in *Reports* in the HP Business Availability Center Documentation Library.
  - Certain System Availability Management reports can be added to custom reports. For details, see “System Availability Management Data in Custom Reports” on page 2100.
  - Data collected by the SiteScope data collector can also be viewed in trend reports. Trend reports enable you to compare multiple measurements from different data sources on the same graph. For details, see “Trend Report Wizard” in *Reports* in the HP Business Availability Center Documentation Library.
  - To avoid affecting the correctness of system availability data during the Daylight Savings Time change (forward or backward), we recommend defining downtime or scheduling an event during the time change period. For more information on scheduling Downtime and Events, see “Downtime/Event Scheduling” in *Platform Administration* in the HP Business Availability Center Documentation Library.
  - If a SiteScope contains many measurements, report generation can take a few minutes.
-



The following System Availability Management reports are available (click the report name for details on the report):

Report	Description
Monitor Performance Report	Displays the best- or worst-performing SiteScope monitors across various SiteScope categories.
Cross-Performance Report	Displays data from more than one SiteScope server filtered by monitored servers, monitor types, and measurements.
Group Performance Report	Displays the infrastructure machine resource usage data for the monitors in the selected group and its subgroups.
Status Summary Report	Displays a quick snapshot of the performance of monitored infrastructure machines, organized by SiteScope group.
Warning Summary Report	Displays a list of the monitors, for the selected group and its subgroups, whose measurements fell within the minor threshold level during the selected time period.
Error Summary Report	Displays a list of the monitors, for the selected group and its subgroups, whose measurements fell within the critical threshold level during the selected time period.

## Understanding the Cross-Performance Report Scale

Measurement values in the cross-performance report are displayed along the y-axis using a normalized scale. By default, HP Business Availability Center automatically sets the scale factor for each measurement. If required, you can manually modify the scale factor for any measurement in the Selected Measurements table, for example, to better view multiple measurements whose data values span a wide range. For details, see “Rescale a Cross-Performance Report” on page 2104.

When you manually modify the scale factor, HP Business Availability Center scales measurement values by dividing the actual value by the value chosen in the scale list. Thus, a value of 100 with a scale setting of 0.1 is shown as 1000 along the y-axis. A value of 100 with a scale setting of 10 is shown as 10 along the y-axis.

### **Rescaling a Cross-Performance Report**

Cross-performance reports are generally scaled so that the lowest y-axis value is zero and the highest y-axis value is the highest result of the data.

You can rescale the report to make it more relevant to the measurement. For example, to measure CPU utilization, you can rescale the report so that the y-axis range is 0 to 100.

For details on rescaling a Cross-Performance report, see “Rescale a Cross-Performance Report” on page 2104.

## Understanding the Group Performance Report

You create the Group Performance report and its subreports to view data that helps you spot trends in server performance that could lead to application performance problems. You can also analyze whether slow or failed transactions are being caused by server resource bottlenecks or other infrastructure machine-related problems.

The Group Performance table is the top level of the report. For each group, the table displays a color-coded quality level, the number of subgroups, and the number of included measurements. The quality-level indicators enable you to see how monitors in the defined groups are performing.

The Group Performance report contains the following sub-reports:

- “SiteScope Performance Report” on page 2099
- “SiteScope Data Over Time Report” on page 2099

### **SiteScope Performance Report**

The SiteScope Performance subreport displays a list of measurements collected by SiteScope for the specified group, over the selected time range. If the specified group contains subgroups, these are displayed at the top of the page. For details, see “SiteScope Performance Report” on page 2116.





### **SiteScope Data Over Time Report**





The SiteScope Data Over Time report displays specific measurement data over the selected time range. You can view this report for a single measurement, or for several measurements simultaneously. For details, see “SiteScope Data over Time Report” on page 2119.

## System Availability Management Data in Custom Reports

You can add System Availability Management reports to custom reports from the Report Manager. For details, see “Custom Report Wizard” in *Reports* in the HP Business Availability Center Documentation Library.

The following table describes how to add System Availability Management reports to custom reports:

Report	To Add to a Custom Report
Monitor Performance Report	Select Applications > User Reports > Report Manager, click <b>New</b>  , select <b>New Custom Report</b> and on the Report Components page, click <b>Add New Component</b>  and Select <b>System Availability Management &gt; SiteScope Monitor Performance</b> from the <b>Select Component Category</b> pane.
SiteScope Data over Time Report	Select Applications > User Reports > Report Manager, click <b>New</b>  , select <b>New Custom Report</b> and on the Report Components page, click <b>Add New Component</b>  and Select <b>System Availability Management &gt; SiteScope Reports</b> . In the Select Component pane, select <b>SiteScope Data Over Time</b> in the Type list.

Report	To Add to a Custom Report
Group Performance Report	Select Applications > User Reports > Report Manager, click <b>New</b>  , select <b>New Custom Report</b> and on the Report Components page, click <b>Add New Component</b>  and Select <b>System Availability Management &gt; SiteScope Reports</b> . In the Select Component pane, select <b>SiteScope Profile Summary</b> in the Type list.
Overall Performance Report	Select Applications > User Reports > Report Manager, click <b>New</b>  , select <b>New Custom Report</b> and on the Report Components page, click <b>Add New Component</b>  and Select <b>System Availability Management &gt; SiteScope Reports</b> . In the Select Component pane, select <b>SiteScope Data Over Time</b> in the Type list.

## Create a Monitor Performance Report – Workflow

This task describes how to specify the criteria on which you want the Monitor Performance Report to be based and create the report.

**To create a Monitor Performance report:**

- 1** Access the Monitor Performance report: Select **Applications > System Availability Management > SiteScope Over Time Reports > Monitor Performance**.
- 2** Click **Profile(s)** and select the SiteScope for which you want to view the report.
- 3** In the **Monitor title** and **Server name** boxes, specify the monitors (by their title, as defined in SiteScope) and servers on which you want the custom report data to be based.

Leave a box empty to instruct HP Business Availability Center to base the report on all values.

If required, you can use the wildcard asterisk symbol (\*) to instruct HP Business Availability Center to base the report on a subset of all values. For example, if you are using the naming convention `cpu_<servername>` to name all CPU monitors in SiteScope, specify `cpu*` to instruct HP Business Availability Center to include all CPU monitors in the custom report.

---

**Note:** Using the wildcard asterisk symbol (\*) as the first character in the string slows report generation times, as HP Business Availability Center is unable to use the Index tables when querying the database.

---

- 4** From the **Monitor type** list, select the monitor on which you want the report data to be based. To base the report on all monitors, choose **All types**.
- 5** Specify whether you want HP Business Availability Center to display the worst- or best-performing monitors, and choose the number of monitors to be displayed in the report.
- 6** Click **Generate** to create the report.

## Create a Cross-Performance Report – Workflow

This task describes how to create a Cross-Performance report.

This task includes the following steps:

- “Access the Cross-Performance Report” on page 2103
- “Select the Time Range and Granularity” on page 2103
- “Select Measurements for Monitoring” on page 2104
- “Configure Scale Report Information” on page 2104
- “Generate and Format the Report” on page 2104

### 1 Access the Cross-Performance Report

Access the Cross-Performance report: Select **Applications > System Availability Management > SiteScope Over Time Reports > Cross-Performance**.

### 2 Select the Time Range and Granularity

Select the time period and the granularity with which you want to run the report. For details on how to perform this task, see “Time Range and Granularity Bar” in *Reports* in the HP Business Availability Center Documentation Library.

---

**Note:** In certain reports the selected time range is displayed along the x-axis. System Availability Management breaks down the time range according to segments, which differ depending on the selected time range. For details on how System Availability Management breaks down each time range in reports where time is displayed along the x-axis, see “Report Times” in *Reference Information* in the HP Business Availability Center Documentation Library.

---

### 3 Select Measurements for Monitoring

Click the **Select Measurements** link to choose the measurements you want the Cross-Performance report to monitor. For details on selecting measurements, see “Select Measurements Dialog Box” on page 2112.

### 4 Configure Scale Report Information

If required, enter scale information in the **Scale Min** and **Max** boxes. For details on performing this task, see “Rescale a Cross-Performance Report” on page 2104.

### 5 Generate and Format the Report

Click **Generate** to create the report. The filter area of the page closes and the report opens.

You can print the report, send it by email, or open it in CSV or PDF format. For details on formatting a report, see “Format Menu Options” in *Reports* in the HP Business Availability Center Documentation Library.

## Rescale a Cross-Performance Report

This task describes how to change the y-axis scale of a Cross-Performance report.

To rescale a Cross-Performance report:

- 1 Click the **Select Measurements** link on the Cross-Performance report page to open the Select Measurements dialog box.
- 2 Specify a minimum, a maximum, or both a minimum and a maximum value in the **Scale Min** and **Max** boxes.

## System Availability Management Reports User Interface

**This section includes:**





- Monitor Performance Report on page 2105



- Cross-Performance Report on page 2109
- Group Performance Report on page 2114
- SiteScope Performance Report on page 2116
- SiteScope Data over Time Report on page 2119
- Status Summary Report on page 2122
- SiteScope Uptime Summary Report on page 2124
- Warning Summary Report on page 2125
- SiteScope Warning Details Report on page 2127
- Error Summary Report on page 2130
- SiteScope Error Details Report on page 2132
- Overall Performance Report on page 2135

## Monitor Performance Report

This is an example of a Monitor Performance report:

Monitor Performance							
<b>Profile(s):</b> AutoSa...profile, AutoSa...lab.ad		<b>Monitor title:</b> <input type="text"/> <b>Server name:</b> <input type="text"/> Use * for wildcard search	<b>Monitor type:</b> All types Show the 5 worst performing monitors	   			
Monitor Title	Server Name	Group	Profile Name	Minor	Critical	Total Runs	Quality
Cpu monitor on ...1ss04.devlab.ad	labm1ss04	<a href="#">Unix monitors f...1ss04.devlab.ad</a>	AutoSanity_SiteScope_On_labm1amrnd19.devlab.ad	0%	100%	7	<div style="width: 100%; height: 10px; background-color: red;"></div>
Cpu monitor on ...1ss08.devlab.ad	labm1ss08.devlab.ad	<a href="#">Windows monitor...1ss08.devlab.ad</a>	AutoSanity_SiteScope_On_labm1amrnd19.devlab.ad	0%	47.06%	17	<div style="width: 47.06%; height: 10px; background-color: red;"></div>
CPU Utilization.../06/05_09:45:26	labm1amr...evlab.ad	<a href="#">Basic_2008/06/05_09:45:26</a>	AutoSanity_SiteScope_On_labm1amrnd19.devlab.ad	0%	1.52%	66	<div style="width: 100%; height: 10px; background-color: green;"></div>
CPU Utilization.../06/05_09:53:00	labm1amr...evlab.ad	<a href="#">Basic_2008/06/05_09:53:00</a>	AutoSanity_SiteScope_On_labm1amrnd19.devlab.ad	0%	1.52%	66	<div style="width: 100%; height: 10px; background-color: green;"></div>
CPU Utilization.../06/05_09:45:26	labm1amr...evlab.ad	<a href="#">Basic_2008/06/05_09:45:26</a>	AutoSanity_Empty_Profile	0%	0%	2	<div style="width: 100%; height: 10px; background-color: green;"></div>

<p><b>Description</b></p>	<p>Displays the best- or worst-performing SiteScope monitors across various SiteScope categories, such as monitor type, monitored server, or monitor title. You can create a Monitor Performance report for multiple SiteScope profiles.</p> <p><b>To access:</b> Select <b>Applications &gt; System Availability Management &gt; SiteScope Over Time Reports &gt; Monitor Performance</b></p>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>➤ Monitors are sorted in the report by quality, which is derived using a formula that takes into account the measurement values returned for the monitor during the specified time range relative to the measurement threshold ranges configured in SiteScope.</li> </ul> <p>The formula used is: <math>1 - ((0.35 * W + 0.5 * E) / (G + W + E))</math>, where G, W, and E represent the number of measurements that occurred during the selected time range whose value was within the OK, Warning, and Error threshold range, respectively. The formula returns values from 0.5 to 1, inclusively. The better a monitor performs, the closer its value is to 1. For example, a monitor with 25% error and 75% OK values would be displayed as better than a monitor with 100% Warning values.</p> <ul style="list-style-type: none"> <li>➤ All data in the report is based on aggregated data. The Monitor Performance report does not use raw data.</li> </ul>
<p><b>Included in Tasks</b></p>	<p>“Create a Monitor Performance Report – Workflow” on page 2102</p>
<p><b>Useful Links</b></p>	<p>“SiteScope Over Time Reports” on page 2095</p>

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .
Monitor Title	Specify the monitors (by their title, as defined in SiteScope) on which you want the custom report data to be based.
Monitor Type	Select the monitor on which you want the report data to be based. To base the report on all monitors, choose <b>All types</b> .
Server Name	Specify the servers on which you want the custom report data to be based.
Show the <number and performance level> monitors	Specify whether you want HP Business Availability Center to display the worst- or best-performing monitors, and choose the number of monitors to be displayed in the report.

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Critical	The percentage of measurement instances that return a critical-level threshold status.
Group	The group or subgroup in which the monitor is defined. Hover over the selected entry to view the path from the displayed group or subgroup to the root group. Click the group or subgroup name to open the management page for the group in SiteScope.
Minor	The percentage of measurement instances that return a minor-level threshold status.

GUI Element (A-Z)	Description
<b>Monitor Title</b>	The title of the SiteScope monitor. Hover over the entry to view a tooltip with the full monitor title.
<b>Profile Name</b>	The name of the SiteScope profile in which the monitor is defined.
<b>Quality</b>	A color-coded representation of quality. Hover over the color to view a tooltip with the exact percentage for each colored section of the bar.  For an explanation of the indicated colors, see “Color Coding in Reports” on page 2108.
<b>Server Name</b>	The name of the monitored server. Hover over the selected entry to view a tooltip with the full server name.
<b>Total Runs</b>	The total number of measurement instances SiteScope ran for the selected time range.

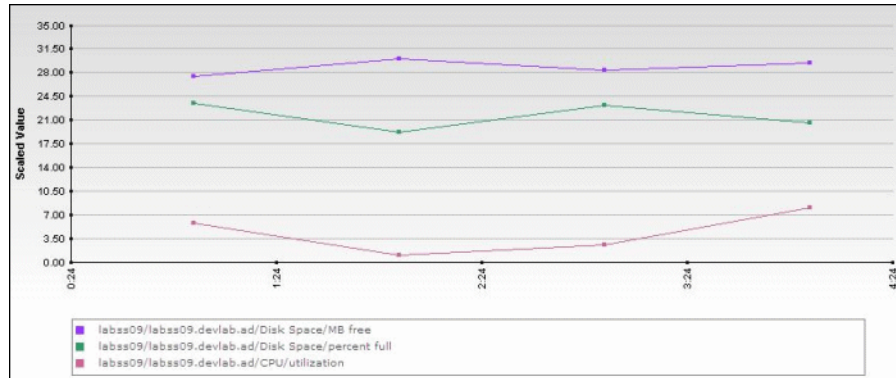
### Color Coding in Reports

System Availability Management reports use the following colors when displaying color-coded performance levels:

Color	Description
<b>Green</b>	All measurements fell within the OK threshold range.
<b>Yellow</b>	At least one measurement fell within the minor threshold range, but no measurements fell within the critical threshold range.
<b>Red</b>	At least one measurement fell within the critical threshold range.
<b>Gray</b>	No measurement data reported.

## Cross-Performance Report

This is an example of a Cross-Performance report:



<b>Description</b>	<p>Displays data from more than one SiteScope server filtered by monitored servers, monitor types, and measurements.</p> <p><b>To access:</b> Select <b>Applications &gt; System Availability Management &gt; SiteScope Over Time Reports &gt; Cross-Performance</b></p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>➤ Click the appropriate tab to choose how you want to view the Cross-Performance report:             <ul style="list-style-type: none"> <li>➤ View as Graph</li> <li>➤ View as Table</li> </ul> </li> <li>➤ You can choose to view data in separate graphs for each measurement, or in one graph for all measurements. For details, see “Select Measurements Dialog Box” on page 2112.</li> </ul>
<b>Included in Tasks</b>	<p>“Create a Cross-Performance Report – Workflow” on page 2103</p>

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .
Select Measurements	Click to open the Select Measurements dialog box and filter the data you want to include in the report. For details, see “Select Measurements Dialog Box” on page 2112.  <b>Note:</b> You cannot create a report if you have not selected at least one measurement.

## Report Content as Graph

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<data points>	Indicate one of the following: <ul style="list-style-type: none"> <li>▶ A change in the data value or measurement frequency from the previous time point on the graph.</li> <li>▶ One hour has passed since the last change in data value or measurement frequency.</li> </ul>
<graph lines>	The value of the specified measurements, at the indicated time. A straight line indicates the following: <ul style="list-style-type: none"> <li>▶ There has been no change in the value of the incoming data from the previous time point on the graph.</li> <li>▶ There has been no change in the frequency that the incoming data is measured in since the previous time point on the graph.</li> </ul> <b>Note:</b> A gap in the graph indicates that no data has been retrieved for the specific time period.

GUI Element (A-Z)	Description
<x-axis>	<p>Displays the date and time of the monitored measurements.</p> <p><b>Note:</b> Depending on the time range you select, System Availability Management generates reports using either raw data or aggregated data. The text: <b>Note: Report uses aggregated data</b> is displayed in the report when aggregated data is used. For details on how System Availability Management determines when to use aggregated data, see “Data Aggregation” in <i>Reference Information</i> in the HP Business Availability Center Documentation Library.</p>
<y-axis>	<p>Displays the measurement values and the monitor type or title, depending on whether you selected <b>Filter by Monitor Type</b> or <b>Filter by Monitor Title</b> in the Select Measurements dialog box.</p>

### Report Content as Table


The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<date>	<p>The date and time of the measurements’ data.</p> <p><b>Note:</b> Depending on the time range you select, System Availability Management generates reports using either raw data or aggregated data. The text: <b>Note: Report uses aggregated data</b> is displayed in the report when aggregated data is used. For details on how System Availability Management determines when to use aggregated data, see “Data Aggregation” in <i>Reference Information</i> in the HP Business Availability Center Documentation Library.</p>
<value>	The value of the specific measurement.
<b>Measurement Name</b>	<p>The name of the measurement, including the server on which it is running.</p> <p><b>Tooltip:</b> Displays the full path of the measurement name.</p>

## Select Measurements Dialog Box

<b>Description</b>	Enables you to filter the data you want to include in the Cross-Performance report. <b>To access:</b> Click the <b>Select Measurements</b> link on the Cross-Performance report page.
<b>Important Information</b>	If you select a measurement for which data exists from more than one group or profile for the same target server, the data is averaged together in the report. For example, if you have two SiteScope profiles each containing two groups, and in three of those groups the Ping monitor is set up to monitor the same server, if you select both profiles and the round trip time measurement, all round trip time data collected from all three groups in both profiles is displayed in the report as an average value.
<b>Included in Tasks</b>	“Create a Cross-Performance Report – Workflow” on page 2103

The following elements are included (unlabeled GUI elements are shown in angle brackets>):
















GUI Element (A-Z)	Description
	Click to list all the elements whose name includes the string entered in the <b>Contains</b> box.
<b>Contains</b>	Optionally, enter a string by which you want to filter elements in the selected column.
<b>Disable auto-scale</b>	Click to disable automatic rescaling of the report scale factor. For details on changing the report scale, see “Understanding the Cross-Performance Report Scale” on page 2098.
<b>Filter by Monitor Title</b>	Select to display the monitor title when choosing the component to add to the report. <b>Example:</b> myserver, CPU finance_server
<b>Filter by Monitor Type</b>	Select to display the monitor type when choosing the component to add to the report. <b>Example:</b> Ping, CPU



GUI Element (A-Z)	Description
<b>Graph per measurement</b>	<p>Select to display a separate graph for each measurement. The graph legend displays the server on which the measurement is running.</p> <p>If de-selected, a new graph is created for each measurement with the title &lt;server_name&gt; <b>continued</b>.</p> <p><b>Default Value:</b> Selected</p>
<b>Measurements</b>	<p>Select one or more measurements. The list includes the measurements that are associated with the selected profiles, servers, and monitor types, in alphabetical order.</p>
<b>Monitor Types/Monitor Measurements</b>	<p>Depending on whether you chose <b>Filter by Monitor Type</b> or <b>Filter by Monitor</b>, displays monitor types or monitor names, associated with the selected profiles and servers, in alphabetical order. Select one or more monitors.</p>
<b>Profiles</b>	<p>Select one or more SiteScope profiles to be included in the report.</p> <p><b>Note:</b> The number of selected profiles are calculated after you click <b>Generate</b>. You can choose up to 10 profiles. If these numbers exceed the allowed limit, an error message is displayed.</p>
<b>Scale</b>	<p>Optionally, enter relevant values in the <b>Min</b> and <b>Max</b> boxes to rescale the y-axis for the report. For details, see “Rescale a Cross-Performance Report” on page 2104.</p> <p><b>Note:</b> If the data values of a monitor are outside the minimum or maximum configured values of the graph, the data points are displayed outside the boundaries of the graph.</p>
<b>Servers</b>	<p>Select one or more servers. The list includes all monitored servers associated with the selected profiles, in alphabetical order.</p>

## Group Performance Report

This is an example of a Group Performance report:

Group Name	Number Of Subgroups	Number Of Measurements		No data
 EMS	0	6		OK
 <a href="#">AutoSanityDeployedTe... 2008/06/03 06:26:10</a>	3	0		Minor
 <a href="#">AutoSanity Integrati... 2008/06/03 06:28:32</a>	1	0		Critical
 <a href="#">AutoSanity Integrati... 2008/06/03 06:43:07</a>	1	0		
 Health	0	0		
 AutoSanity	1	0		
 <a href="#">AutoSanity 2008/06/03 06:24:21</a>	1	0		

**Note:** Report uses hourly aggregated data.

<b>Description</b>	<p>Displays the infrastructure machine resource usage data for the monitors in the selected group and its subgroups.</p> <p>You use this report to view data that helps you spot trends in server performance that could lead to application performance problems.</p> <p><b>To access:</b> Select <b>Applications &gt; System Availability Management &gt; SiteScope Over Time Reports &gt; Group Performance</b></p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ The Group Performance Report contains the following sub-reports:                             <ul style="list-style-type: none"> <li>▶ SiteScope Performance Report</li> <li>▶ SiteScope Data Over Time Report</li> </ul> </li> <li>▶ You click the group name to open the SiteScope Performance report for the specified group.</li> </ul>
<b>Useful Links</b>	<p>“SiteScope Performance Report” on page 2116</p> <p>“SiteScope Data over Time Report” on page 2119</p>

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<quality level indicator>	A color-coded icon which enables you to see how monitors in the defined groups are performing. <b>Tooltip:</b> Indicates the group’s quality level and number of critical errors.
<quality level legend>	Indicates the quality level that the colored icons in the Group Performance table represent.
Group Name	The name of the SiteScope monitor group. Click the group name to open the SiteScope Performance report for the specified group. For details on the SiteScope Performance report, see “SiteScope Performance Report” on page 2116. <b>Tooltip:</b> Displays the full group name.
Number of Measurements	The number of measurements contained in the specified group.
Number of Subgroups	The number of subgroups contained in the specified group.

## SiteScope Performance Report

This is an example of a SiteScope Performance report:

SiteScope Measurements for Group: Unix monitors for labm1ss04.devlab.ad						
	Monitor Title	Measurement Name	Host Name	Avg. Value	Critical Errors / Total	
<input checked="" type="checkbox"/>	Memory on labm1ss04.devlab.ad	<a href="#">pages/sec</a>	labm1ss04	0.0	0 / 24	
<input type="checkbox"/>	Memory on labm1ss04.devlab.ad	<a href="#">percent used</a>	labm1ss04	0.0	0 / 24	
<input type="checkbox"/>	Memory on labm1ss04.devlab.ad	<a href="#">MB free</a>	labm1ss04	1992.0	0 / 24	
<input type="checkbox"/>	Cpu monitor on labm1ss04.devlab.ad	utilization	labm1ss04	-	<a href="#">24</a> / 24	

Note: Report uses hourly aggregated data.

<b>Description</b>	<p>Displays a list of measurements collected by SiteScope for the specified group, over the selected time range.</p> <p><b>To access:</b> Click an entry in the Group Name field on the Group Performance table.</p>
<b>Important Information</b>	<p>The SiteScope Performance Report is divided into the following sections:</p> <ul style="list-style-type: none"> <li>▶ <b>Subgroups for Group:</b> &lt;Group name&gt;. The elements displayed in this section are identical to those displayed on the Group Performance report main page.</li> <li>▶ <b>SiteScope Measurements for Group:</b> &lt;Group name&gt;. Displays the measurements collected for the specified group.</li> </ul>

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .
<b>Generate</b>	Click to generate the SiteScope Data Over Time report for the selected measurements.  <b>Note:</b> This button is located underneath the SiteScope Performance report, and is enabled only if there are enabled check boxes in the <b>SiteScope Measurements for Group: &lt;Group name&gt;</b> section.

## Report Content for Subgroups for Group: <Group Name> Table

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<quality level indicator>	A color-coded icon which enables you to see how monitors in the defined groups are performing.  <b>Tooltip:</b> Indicates the group’s quality level and number of critical errors.
<quality level legend>	Indicates the quality level that the colored icons in the Group Performance table represent.
<b>Group Name</b>	The name of the SiteScope monitor group. Click the group name to open the SiteScope Performance report for the specified group’s measurements. For details, see “Report Content for SiteScope Measurements for Group: <Group Name> Table” on page 2118.  <b>Tooltip:</b> Displays the full group name.

GUI Element (A-Z)	Description
<b>Number of Measurements</b>	The number of measurements contained in the specified group.
<b>Number of Subgroups</b>	The number of subgroups contained in the specified group.

### Report Content for SiteScope Measurements for Group: <Group Name> Table

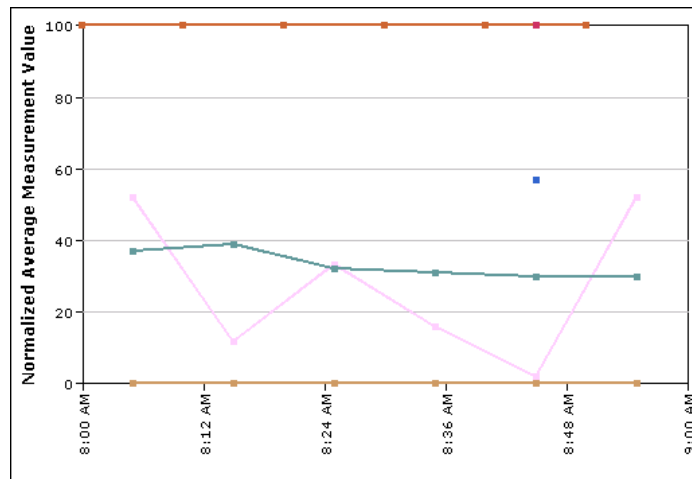
The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<check box>	An enabled check box indicates that there is monitor data that can be viewed in the SiteScope Data Over Time report. To view this data, select the checkbox corresponding to the measurement for which you want to view data, and click <b>Generate</b> .  For details on the SiteScope Data Over Time report, see “SiteScope Data over Time Report” on page 2119.
<quality level indicator>	Displays measurement threshold colored icons, which indicate whether the average measurement is within the OK, Warning, or Error range, as reported by SiteScope. You define measurement thresholds for each measurement when you configure the monitor in the System Availability Management area in the Administration Console. For details, see “Setting Status Thresholds” on page 309.
<b>Avg. Value</b>	The average value of each listed measurement, or counter, for the specified time period.
<b>Critical Errors/Total</b>	The number of critical errors that occurred while collecting measurement data, out of the total number of measurements taken during the defined time period. Click the link to view a list of critical error messages. HP Business Availability Center displays the link only if errors occurred.

GUI Element (A-Z)	Description
Host Name	The name of the SiteScope host machine.
Measurement Name	The name of the measurement. If measurement data exists for the selected time range, the measurement name appears as a link. Click the measurement link to open the SiteScope Data Over Time report. For details on the SiteScope Data Over Time report, see “SiteScope Data over Time Report” on page 2119.
Monitor Title	The title of the monitor.

## SiteScope Data over Time Report

This is an example of a SiteScope Data Over Time report:



<p><b>Description</b></p>	<p>Displays specific measurement data over the selected time range.</p> <p><b>To access:</b> From the SiteScope Performance Report, perform one of the following actions:</p> <ul style="list-style-type: none"> <li>▶ Select the checkbox corresponding to the measurement you want to view data for and click <b>Generate</b>.</li> <li>▶ Click the measurement link in the <b>Measurement Name</b> column. This column displays a link only if there is measurement data exists for the selected time range.</li> </ul>
<p><b>Important Information</b></p>	<ul style="list-style-type: none"> <li>▶ You can view this report for a single measurement, or for several measurements simultaneously.</li> <li>▶ You can add the SiteScope Data over Time report to custom reports. For details, see “Custom Report Wizard” in <i>Reports</i> in the HP Business Availability Center Documentation Library.</li> <li>▶ Click the appropriate tab to view the report either in graph or table format. When viewing in table format, the table displays actual measurement values, not normalized values.</li> </ul>

### Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Format Buttons>	Click the appropriate button to print the report, send it by email, or open it in CSV or PDF format. For details, see “Format Menu Options” in <i>Reports</i> .



## Report Content as Graph

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<color code legend>	Identifies the measurements in the graph, by color.
<data points>	<b>Tooltip:</b> Displays measurement details, including the measurement's original value.
<x-axis>	Displays the date and time of the monitored measurements.
<y-axis>	Displays a normalized scale of 0 - 100 for the monitored measurements. HP Business Availability Center uses the following formula to convert the original y-axis value to a value in the merged y-axis:  [original y-axis value] x [scale value] = y-axis value in merged graph
<b>View as Table</b>	Click to view the SiteScope Data Over Time report in table format.

## Report Content as Table













The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<date>	The date of the data output for the selected measurement.
<monitor title and measurement name>	<b>Tooltip:</b> Hover over the entry to view the title of the monitor being measured, and the name of the specific measurement.  This element is located on the left side of the table.
<time>	The time of the data output for the selected measurement.

GUI Element	Description
<value>	The value of the measurement for the specified time.
<b>View as Graph</b>	Click to view the SiteScope Data Over Time report in graph format.

## Status Summary Report

This is an example of a Status Summary report:

Group Name	Number Of Subgroups	Number Of Measurements	
 <a href="#">EMS</a>	0	6	
 <a href="#">AutoSanityDeployedTe... 2008/06/03 06:26:10</a>	3	0	
 <a href="#">AutoSanity Integrati... 2008/06/03 06:28:32</a>	1	0	
 <a href="#">AutoSanity Integrati... 2008/06/03 06:43:07</a>	1	0	
 <a href="#">Health</a>	0	0	
 <a href="#">AutoSanity</a>	1	0	
 <a href="#">AutoSanity 2008/06/03 06:24:21</a>	1	0	

**Note:** Report uses hourly aggregated data.

<b>Description</b>	<p>Displays a quick snapshot of the performance of monitored infrastructure machines, organized by SiteScope group.</p> <p>You create the Status Summary report and its subreport to get an overall view of the performance of defined SiteScope groups and the monitors defined therein.</p> <p><b>To access:</b> Select <b>Applications &gt; System Availability Management &gt; SiteScope Over Time Reports &gt; Group Performance</b></p>
--------------------	---

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<quality level indicator>	A color-coded icon which enables you to see how monitors in the defined groups are performing. <b>Tooltip:</b> Indicates the group’s quality level and number of critical errors.
<quality level legend>	Indicates the quality level that the colored icons in the Group Performance table represent.
Group Name	The name of the SiteScope monitor group. Click the group name to open the SiteScope Uptime Summary report for the specified group. For details on the SiteScope Uptime Summary report, see “SiteScope Uptime Summary Report” on page 2124. <b>Tooltip:</b> Displays the full group name.
Number of Measurements	The number of measurements contained in the specified group.
Number of Subgroups	The number of subgroups contained in the specified group.

## SiteScope Uptime Summary Report

This is an example of the SiteScope Uptime Summary Report:

SiteScope Uptime for Group: Net_Mon			
Monitor Title	Uptime %	Warning %	Error %
Ping Intranet	88.889	0.0	11.111
Network Interface	100.0	0.0	0.0
Ping: www.freshwater.com	100.0	0.0	0.0

<b>Description</b>	<p>Displays <b>OK</b>, <b>Minor</b>, and <b>Critical</b> information for each monitor in the group, over the selected time range</p> <p>The SiteScope Uptime Summary report enables you to determine the overall performance trend of a given monitor.</p> <p><b>To access:</b> Click a group name in the Status Summary report.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ If the specified group contains subgroups, these are displayed at the top of the page. Click the subgroups to view their SiteScope Uptime Details subreports.</li> <li>▶ This report cannot be opened in PDF format.</li> </ul>

### Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .



## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
<b>Critical %</b>	The percentage of measurement instances whose values fell within the <b>Critical</b> threshold level.
<b>Minor %</b>	The percentage of measurement instances whose values fell within the <b>Minor</b> threshold level.
<b>Monitor Title</b>	The title of the monitor being measured.
<b>OK %</b>	The percentage of measurement instances that completed successfully.

## Warning Summary Report

This is an example of the Warning Summary report:

	Group Name	Number Of Subgroups	Number Of Measurements
	<a href="#">Examples</a>	4	0
	<a href="#">Group1</a>	1	60

<b>Description</b>	<p>Displays a list of the monitors, for the selected group and its subgroups, whose measurements fell within the minor threshold level during the selected time period.</p> <p>You create the Warning Summary report and its subreport to identify the SiteScope groups whose measurements fell within the minor threshold level during the selected time period.</p> <p><b>To access:</b> Select <b>Applications &gt; System Availability Management &gt; SiteScope Over Time Reports &gt; Warning Summary</b></p>
--------------------	---

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<quality level indicator>	A color-coded icon which enables you to see how monitors in the defined groups are performing. <b>Tooltip:</b> Indicates the group’s quality level and number of critical errors.
<quality level legend>	Indicates the quality level that the colored icons in the Group Performance table represent.
Group Name	The name of the SiteScope monitor group. Click the group name to open the SiteScope Warning Details report for the specified group. For details on the SiteScope Warning Details report, see “SiteScope Warning Details Report” on page 2127. <b>Tooltip:</b> Displays the full group name.
Number of Measurements	The number of measurements contained in the specified group.
Number of Subgroups	The number of subgroups contained in the specified group.

## SiteScope Warning Details Report

This is an example of the SiteScope Warning Details report:

Time	Monitor Title	Measurement Name	Status
7/24/04 7:47 AM	alerts	Number o...d Agents	0.0
7/24/04 7:47 AM	alerts	Received...l Alerts	0.0
7/24/04 7:37 AM	alerts	Number o...d Agents	0.0
7/24/04 7:37 AM	alerts	Received...l Alerts	0.0

<b>Description</b>	<p>Displays minor status information for each measurement instance of each monitor in the group, over the selected time range.</p> <p><b>To access:</b> Click a group name in the Warning Summary report.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ System Availability Management displays only raw data in the SiteScope Warning Details report. Aggregated data is not used. Therefore, if raw historical data is removed from the profile database using the Purging Manager, you are unable to view data in the SiteScope Warning Details report for the time period for which the data was removed.</li> <li>▶ This report cannot be opened in PDF format.</li> </ul>

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .

## Report Content for Subgroups for Group: <Group Name> Table

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<quality level indicator>	A color-coded icon which enables you to see how monitors in the defined groups are performing. <b>Tooltip:</b> Indicates the group’s quality level and number of critical errors.
<quality level legend>	Indicates the quality level that the colored icons in the Group Performance table represent.
Group Name	The name of the SiteScope monitor group. Click the group name to open the SiteScope Warning Details report for the specified group and view the group’s measurements. For details, see on the SiteScope Performance report, see “Report Content for SiteScope Warning Measurements for Group: <Group Name> Table” on page 2129. <b>Tooltip:</b> Displays the full group name.
Number of Measurements	The number of measurements contained in the specified group.
Number of Subgroups	The number of subgroups contained in the specified group.


















**Report Content for SiteScope Warning Measurements for Group: <Group Name> Table**

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
<b>Measurement Name</b>	The measurement instance whose threshold fell within the <b>Minor</b> level.
<b>Monitor Title</b>	The monitor to which the measurement is associated.
<b>Status</b>	The value of the measurement.
<b>Time</b>	The date and time of the measurement instance.

## Error Summary Report

This is an example of an Error Summary report:

Group Name	Number Of Subgroups	Number Of Measurements		No data
 EMS	0	6		OK
 <a href="#">AutoSanityDeployedTe... 2008/06/03 06:26:10</a>	3	0		Critical
 <a href="#">AutoSanity Integrati... 2008/06/03 06:28:32</a>	1	0		Minor
 <a href="#">AutoSanity Integrati... 2008/06/03 06:43:07</a>	1	0		Minor
 <a href="#">Health</a>	0	0		No data
 <a href="#">AutoSanity</a>	1	0		No data
 <a href="#">AutoSanity 2008/06/03 06:24:21</a>	1	0		No data

**Note:** Report uses hourly aggregated data.

<p><b>Description</b></p>	<p>Displays a list of the monitors, for the selected group and its subgroups, whose measurements fell within the critical threshold level during the selected time period.</p> <p>You create the Error Summary report and its subreport to identify the SiteScope groups whose measurements fell within the critical threshold level during the selected time period.</p> <p><b>To access:</b> Select <b>Applications &gt; System Availability Management &gt; SiteScope Over Time Reports &gt; Error Summary</b></p>
<p><b>Important Information</b></p>	<p>For each SiteScope group in the selected profile, the report displays a color-coded quality level, the number of subgroups, and the number of included measurements. The quality-level indicators enable you to get a quick snapshot of how monitors in the defined SiteScope groups are performing.</p>

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<quality level indicator>	A color-coded icon which enables you to see how monitors in the defined groups are performing. <b>Tooltip:</b> Indicates the group’s quality level and number of critical errors.
<quality level legend>	Indicates the quality level that the colored icons in the Group Performance table represent.
Group Name	The name of the SiteScope monitor group. Click the group name to open the SiteScope Error Details report for the specified group. For details on the SiteScope Error Details report, see “SiteScope Error Details Report” on page 2132. <b>Tooltip:</b> Displays the full group name.
Number of Measurements	The number of measurements contained in the specified group.
Number of Subgroups	The number of subgroups contained in the specified group.

## SiteScope Error Details Report

This is an example of a SiteScope Error Details report:

Time	Monitor Title	Measurement Name	Status
7/22/04 11:11 PM	IIS on san3	Web Serv...Web Site	Anonymous Use...equests n/a,
7/22/04 11:11 PM	IIS on san3	Web Serv...Web Site	Anonymous Use...equests n/a,
7/22/04 11:11 PM	IIS on san3	Web Serv...c:_Total	Anonymous Use...equests n/a,
7/22/04 11:11 PM	IIS on san3	Web Serv...Web Site	Anonymous Use...equests n/a,

<b>Description</b>	<p>Displays error status information for each measurement instance of each monitor in the group, over the selected time range.</p> <p><b>To access:</b> Click a group name in the Error Summary report.</p>
<b>Important Information</b>	<ul style="list-style-type: none"> <li>▶ System Availability Management displays only raw data in the SiteScope Error Details report. Aggregated data is not used. Therefore, if raw historical data was removed from the profile database using the Purging Manager, you are unable to view data in the SiteScope Error Details report for the time period for which the data was removed.</li> <li>▶ This report cannot be opened in PDF format.</li> </ul>

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .

## Report Content for Subgroups for Group: <Group name> Table

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<quality level indicator>	A color-coded icon which enables you to see how monitors in the defined groups are performing. <b>Tooltip:</b> Indicates the group’s quality level and number of critical errors.
<quality level legend>	Indicates the quality level that the colored icons in the Group Performance table represent.
Group Name	The name of the SiteScope monitor group. Click the group name to open the SiteScope Error Details report for the specified group’s measurements. For details, see “Report Content for SiteScope Error Messages for Group: <Group name> Table” on page 2134. <b>Tooltip:</b> Displays the full group name.
Number of Measurements	The number of measurements contained in the specified group.
Number of Subgroups	The number of subgroups contained in the specified group.

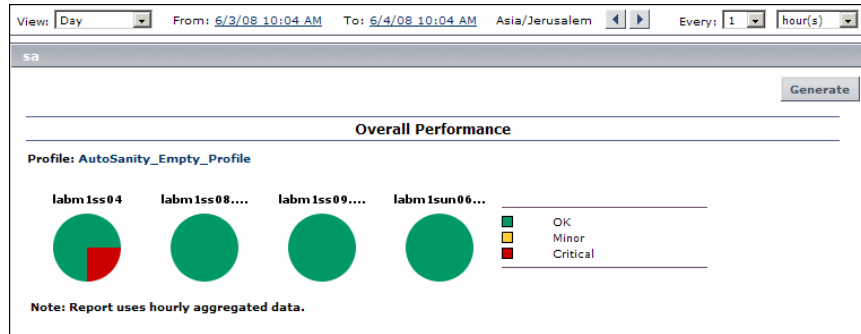
**Report Content for SiteScope Error Messages for Group:  
<Group name> Table**




The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<b>Measurement Name</b>	The measurement instance whose threshold fell within the Error level.
<b>Monitor Title</b>	The monitor to which the measurement is associated.
<b>Status</b>	Error information as reported by SiteScope.
<b>Time</b>	The data and time of the measurement instance.

## Overall Performance Report

This is an example of an Overall Performance report:



<p><b>Description</b></p>	<p>Displays a quick snapshot of the performance of the monitored infrastructure machines in the selected SiteScope profiles.</p> <p><b>To access:</b> Select <b>Applications &gt; User Reports &gt; Report Manager</b>, click <b>New</b> , select <b>New Custom Report</b> and on the Report Components page, click <b>Add New Component</b>  and Select <b>System Availability Management &gt; SiteScope Reports</b> from the <b>Select Component Category</b> pane. In the Select Component pane, select <b>Overall Performance</b> in the Type list.</p> <p><b>To access an existing Overall Performance report:</b> Select the appropriate custom report in the Report Manager and click the <b>View</b> button .</p>
<p><b>Important Information</b></p>	<p>This report is available only in Custom reports, and is not visible on the System Availability Management interface.</p>
<p><b>Useful Links</b></p>	<p>“Custom Reports” in <i>Reports</i></p>

## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
<color code legend>	Identifies the measurement statuses in the graph, by color.
<pie charts>	Represents the performance of each element of the infrastructure that SiteScope is monitoring. <b>Tooltip:</b> Describes the exact number and percentage of measurements for each segment of the chart.
Profile	The profile that is being monitored.



# 160

---

## Event Log

The HP System Availability Management event log displays SiteScope events, as well as events collected from external applications or software by enterprise management systems (EMS) using SiteScope.

---

**Note:** The Event Log is available only to HP Business Availability Center users.

---

### **This chapter includes:**

#### **Concepts**

- ▶ Event Log Overview on page 2138

#### **Tasks**

- ▶ View the Event Log - Workflow on page 2139
- ▶ Customize the Event Log on page 2141
- ▶ Set Additional Filters for SiteScope on page 2142

#### **Reference**

- ▶ Event Log User Interface on page 2142

## Event Log Overview

The Event Log page displays the logs of events that are sent to the system. You can use filters (time frame, data source, severity, and target name) to display specific information. If you select the SiteScope data source, you can then select additional filters: SiteScope profile, groups, and monitor type.

The event log enables you to diagnose specific issues in real time and to create trend reports. For details on creating trend reports, see “Trend Reports” in *Reports* in the HP Business Availability Center Documentation Library.

The event log enables you to view event data over time, events that happened at a specific time, the details of a specific event, and (where possible) the event history.

The type of event that is collected depends on what is defined as an event in the external applications or software. Event types can be warnings, alerts, user logins, and so on.

When you create the event log, the Event Log page displays the events sorted by the time of their occurrence in descending order. It also shows columns that are common to all the data sources that can send events. The data of the SiteScope data source is filtered according to SiteScope Profile permissions (for details, see “Permissions Overview” in *Platform Administration* in the HP Business Availability Center Documentation Library).

The event log displays event data that is common to all data sources, including:

- the severity of the event
- the application or software from which the event is collected
- the time the event occurred
- the hierarchy of the event source
- the name (or the IP address) of the host or device that caused the event
- the status or type of event
- the external system description of the event

You can filter the events for a specific time frame, data source, severity, and target name. For details, see “View the Event Log - Workflow” on page 2139.

Once the events are filtered, you can drill down to the common data to:

- ▶ display data that is specific to the data source where the event occurred. For details on this topic, see “Event Details Page” on page 2148.
- ▶ display the history of a specific event. For details on this topic, see “Event History Page” on page 2149.

## View the Event Log - Workflow

This task describes how to view the logs of events sent to HP Business Availability Center.

This task includes the following steps:

- ▶ “Prerequisites” on page 2139
- ▶ “Select the Event Log Time Period” on page 2140
- ▶ “Edit Filters in the Active Filters Dialog Box” on page 2140
- ▶ “Format the Event Log” on page 2140

### 1 Prerequisites

Make sure that SiteScopes are configured to monitor the infrastructure of your HP Business Availability Center system. Select **Admin > System Availability Management** and verify that there are hosted SiteScopes in the <left pane> by hovering over the entries, and view the information presented on the resulting tooltip.

For details on configuring SiteScopes in HP Business Availability Center, see “Collect Data on the Performance of an IT Resource” on page 164.

## **2 Select the Event Log Time Period**

Select **Applications > System Availability Management > Event Log** to display the Event Log page. In the **View** list, select the time period for which you want to gather information to display in the report.

For details on how to perform this task, see “Time Range and Granularity Bar” in *Reports* in the HP Business Availability Center Documentation Library.

## **3 Edit Filters in the Active Filters Dialog Box**

Optionally, you can click the **Active Filters** link to edit the filters for the events to be displayed on the Events Log page.

For details, see “Active Filters Dialog Box” on page 2147.

## **4 Format the Event Log**

Optionally, click one of the action buttons to print, email, or open a report in Excel or PDF format.

For details on how to perform this task, see “Format Menu Options” in *Reports* in the HP Business Availability Center Documentation Library.

## Customize the Event Log

This task describes how to customize the Event Log.

This task includes the following steps:

- “Change the Maximum Number of Rows Displayed in a Page” on page 2141
- “Configure History View for Data Sources” on page 2141

### 1 Change the Maximum Number of Rows Displayed in a Page

When there are too many events to display in one page of a table, you may want to modify the number of rows permitted on a page.

- a Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **End User/System Availability Management**, and locate the **Max Table Rows** in the **Event Reports** table.
- b Modify the value to the required number of rows per page.

### 2 Configure History View for Data Sources



You can enable the **History** button for selected data sources by configuring the relevant parameters in the Infrastructure Settings.

- a Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Applications**, select **End User/System Availability Management**, and in the **End User/System Availability Management - Data** table, locate the **Event Log Report Data Sources History** entry.
- b In the **Value** box, set the property value by adding the data source names for which you want to enable the **History** button. Separate multiple data source names with commas.



The change takes effect after restart.

## Set Additional Filters for SiteScope

If you select a SiteScope data source in the active filter, an additional filter is automatically provided to filter the data by SiteScope profile, group, and monitor type.

**To work with additional filters for SiteScope data sources:**

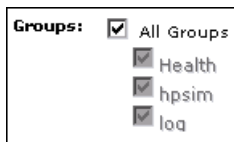
- 1** Click **SiteScope Filters**, to open the **SiteScope Filter** page.
- 2** Select the type of monitor in the **Monitor Type** list. The default is **All Monitor Types**.
- 3** Select the SiteScope profile in the **Profile** list. The default is **All Profiles**. To view events of interest regarding the profile or group permissions, select one of the profiles in the **Profile** list. The list of groups allowed for the selected profile is displayed. For details on profile or group permissions, see “Permissions Overview” in *Platform Administration* in the HP Business Availability Center Documentation Library.

---

**Note:** If you select **All Profiles**, your profile or group permissions are not applied to the displayed events.

---

- 4** If available, select the required group in the group tree. Select **All Groups** if you want to select all the groups in the tree. When a tree CI changes its status (from selected to unselected or from unselected to selected) the status of the whole sub-tree changes.



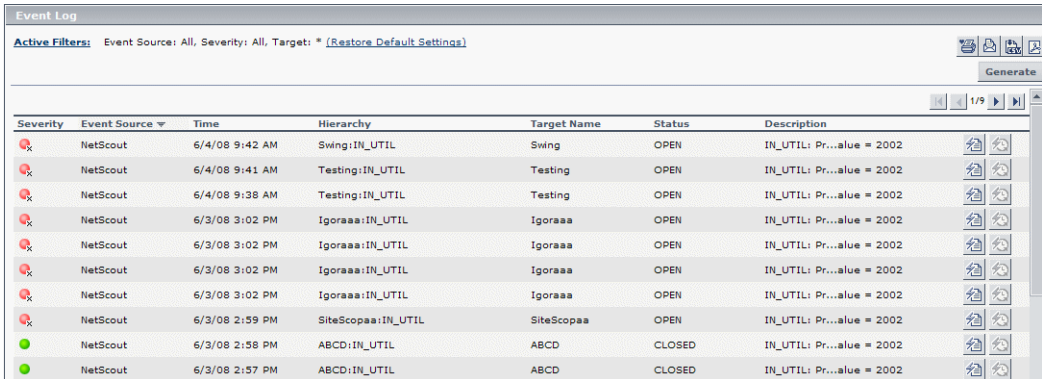
## Event Log User Interface

**This section includes:**











- Event Log Page on page 2143

## Event Log Page

This is an example of the Event Log:



The screenshot shows the Event Log interface with the following data:

Severity	Event Source	Time	Hierarchy	Target Name	Status	Description
	NetScout	6/4/08 9:42 AM	Swing:IN_UTIL	Swing	OPEN	IN_UTIL: Pr...alue = 2002
	NetScout	6/4/08 9:41 AM	Testing:IN_UTIL	Testing	OPEN	IN_UTIL: Pr...alue = 2002
	NetScout	6/4/08 9:38 AM	Testing:IN_UTIL	Testing	OPEN	IN_UTIL: Pr...alue = 2002
	NetScout	6/3/08 3:02 PM	Igoraaa:IN_UTIL	Igoraaa	OPEN	IN_UTIL: Pr...alue = 2002
	NetScout	6/3/08 3:02 PM	Igoraaa:IN_UTIL	Igoraaa	OPEN	IN_UTIL: Pr...alue = 2002
	NetScout	6/3/08 3:02 PM	Igoraaa:IN_UTIL	Igoraaa	OPEN	IN_UTIL: Pr...alue = 2002
	NetScout	6/3/08 3:02 PM	Igoraaa:IN_UTIL	Igoraaa	OPEN	IN_UTIL: Pr...alue = 2002
	NetScout	6/3/08 2:59 PM	SiteScopaa:IN_UTIL	SiteScopaa	OPEN	IN_UTIL: Pr...alue = 2002
	NetScout	6/3/08 2:58 PM	ABCD:IN_UTIL	ABCD	CLOSED	IN_UTIL: Pr...alue = 2002
	NetScout	6/3/08 2:57 PM	ABCD:IN_UTIL	ABCD	CLOSED	IN_UTIL: Pr...alue = 2002

<b>Description</b>	<p>Displays the event data common to all event data sources. The Event Log displays SiteScope events, as well as events collected from external applications or software by enterprise management systems (EMS) using SiteScope.</p> <p><b>To access:</b> Select <b>Applications &gt; System Availability Management &gt; Event Log</b></p>
<b>Important Information</b>	<p>If the number of events that occur during the specified time frame is larger than the maximum number of events that can be displayed in the report, a message is displayed indicating this. To reduce the number of events, select a more specific time range. For example, to see events for the past week, select the individual days of the week.</p>



## Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets>):







GUI Element (A-Z)	Description
<Common report settings>	For details on the user interface, see “Common Report Elements” in <i>Reports</i> .
<b>Active Filters</b>	Enables you to set filters on event log components, to pinpoint the specific events you most want to view. For details on Active Filters, see “Active Filters Dialog Box” on page 2147.  <b>Note:</b> You can click a value in a specific row to add that value to the active filter.

## Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
	Click to open the Event Details page and view additional data for the event. For details, see “Event Details Page” on page 2148.
	Click to open the Event History page and view details about the event history data. For details, see “Event History Page” on page 2149.
<b>Description</b>	The event description. If the description is very long, the value is shortened and the tooltip displays the full hierarchy.
<b>Event Source</b>	The application or software from which the event is collected. For a list of possible event sources, see “Event Sources” on page 2146.



GUI Element (A-Z)	Description
<b>Hierarchy</b>	<p>The hierarchy description of the event source. It can include the path to where the event occurred in the area, sub area, or instance and/or the event depending on the application or software from which the event is collected. The hierarchy can have two to four branches, depending on the data source. If the hierarchy is very long, this field displays the shortened string and the tooltip displays the complete hierarchy.</p>
<b>Severity</b>	<p>A colored icon indicating the severity level of the event.</p> <ul style="list-style-type: none"> <li>➤  . Unknown</li> <li>➤  . Informational</li> <li>➤  . Warning</li> <li>➤  . Minor</li> <li>➤  . Major</li> <li>➤  . Critical</li> </ul> <p><b>Tooltip:</b> Displays the severity of the event.</p>
<b>Status</b>	<p>The status or type of the event. If the hierarchy is very long, the value is shortened and the tooltip displays the full hierarchy.</p>
<b>Target Name</b>	<p>The name or the IP address of the host or device that caused the event.</p>
<b>Time</b>	<p>The time when the event occurred. By default, the data sorted in this column is in descending order.</p>

### **Event Sources**

Following are the applications and software from which events can be collected, depending on the external systems that sent the events to HP Business Availability Center:

- HP OVO
- Remedy ARs
- SitescopeAlert
- SitescopeAlertStatusChange
- Tivoli TEC
- BMC Patrol
- CA Unicenter
- HP SIM
- Compaq Insight Manager
- Whatsup
- Compaq Insight Manager


 **Active Filters Dialog Box**

<b>Description</b>	<p>Enables you to set filters on specific event log fields, to pinpoint the events you most want to view.</p> <p><b>To access:</b> Click the <b>Active Filters</b> link in on the Event Log Page.</p>
--------------------	---

The Active Filters dialog box includes the following filter tabs and areas:

<b>GUI Element (A-Z)</b>	<b>Description</b>
<b>Event Source</b>	<p>Enables you to filter the data displayed in the Event Log according to specific event sources.</p> <p>The Event Source tab includes the following options:</p> <ul style="list-style-type: none"> <li>▶ <b>All</b>. Click to view all event sources in the Event Log page.</li> <li>▶ <b>&lt;Event Source Name&gt;</b>. Click to view only the specified event source in the Event Log page.</li> </ul>
<b>Severity</b>	<p>Enables you to filter the data displayed in the Event Log according to event severity level.</p>
<b>Target</b>	<p>Enables you to filter the data displayed in the Event Log according to target location.</p> <p><b>Note:</b> To view all targets, enter an asterisk in the <b>Targets</b> field.</p>

## Event Details Page



<b>Description</b>	<p>Displays detailed information about the specified event as well as the fields and the field values from the event data.</p> <p><b>To access:</b> Click the <b>Event Details</b> button  on the Event Log page next to the event from which you want to retrieve information.</p>
<b>Important Information</b>	The type of information provided depends on the data source. Not all elements are displayed for all events.

The following elements are included (unlabeled GUI elements are shown in angle brackets>):

GUI Element (A-Z)	Description
<b>Acknowledged By</b>	The operator who acknowledged the event.
<b>Collector Host IP</b>	The IP address of the machine that collected the data.
<b>Collector Host Name</b>	The name of the machine that collected the data.
<b>Description</b>	A description of the event.
<b>Event Source</b>	The application or software from which this event is collected.
<b>Group</b>	The additional logical level of event hierarchy.
<b>Hierarchy</b>	<p>The hierarchy of the event source. It can include the path to where the event occurred in the area, sub area, or instance and/or the event depending on the application or software from which the event is collected.</p> <p>Depending on the data source, the hierarchy can have two to four branches. If the hierarchy is very long, this field displays the shortened string and the tooltip displays the complete hierarchy.</p>
<b>Original Severity</b>	The original severity of the event.
<b>Severity</b>	The severity of the event.
<b>Status</b>	The event status or type.

GUI Element (A-Z)	Description
Target Name	The name of the host or device that caused the event.
Time	The time of the event.
Value	Any numeric values that are sent with the event.

## Event History Page

<b>Description</b>	<p>Displays detailed information about the specified event for different time periods.</p> <p>You use the event history report to receive a historical view of the event.</p> <p><b>To access:</b> Click the <b>Event History</b> button  on the Event Log page.</p>
<b>Important Information</b>	<p>The elements displayed in the Event History page are identical to those displayed on the Event Log page. However, you cannot view the event details report from the Event History page, as the <b>Event Details</b> button  is not displayed.</p>



---

# Index

## A

- Absolute Schedule page 1490
- Absolute Schedule Preferences 1488
- accessing SiteScope 40
- Acknowledge dialog box 1867
- acknowledgements
  - events 105
  - monitor status 105
- Activate Baseline dialog box 389
- activating a baseline 314
- Active Directory
  - monitoring solution 1673
- Active Directory monitor 407
- Active Directory solution template
  - deploying 1675
- adaptors
  - adding SiteScope UNIX adaptors 1364
  - SiteScope UNIX adaptor command list 1367
  - SiteScope UNIX adaptor file format 1366
  - SiteScope UNIX adaptors 1363
  - SiteScope UNIX default adaptor file list 1365
- Add Items dialog box 460
- Adherence level, setting 317
- adherence levels, fine-tuning 387
- administrator, login account 45
- Advanced Filter dialog box, Global Search and Replace 187
- Affected Objects page, Global Search and Replace 186
- agentless SSH, monitors supported by 1341
- aggregation 2093
- AIX Host solution template
  - deploying 1681
- AIX Host, monitoring solution 1679
- Alert action 2006
- alert actions, creating 1963
- Alert log 1956
- Alert report
  - Alert Report Settings 2071
  - example 2072, 2083
  - Report Targets 2070
- Alert Report dialog box 2070
- Alert Settings, Infrastructure Preferences 1403
- Alert templates
  - customizing 1969
  - customizing alert messages 1986
- Alerts
  - Alert Action dialog box 2006
  - customizing alert template message content 1986
  - customizing alert template tag styles 1988
  - customizing alert templates 1969
  - templates directory 1989
- alerts
  - configuring 1984
  - copying and pasting 1984
  - creating 1984
  - creating alert actions 1963
  - customizing message content 1986
  - database 1971
  - editing 1605, 1608, 1998, 2000
  - Email 1973
  - enable-disable monitor 1972
  - Log Event 1974
  - Pager 1975
  - Post 1976
  - script 1977
  - SMS 1981
  - SNMP Trap 1982

## Index

- sound 1983
- Status Trigger panel 2024
- table of, in reports 2049, 2063
- testing 1985
- Trigger Frequency panel 2025
- triggering 1964
- understanding 1960
- Alerts table, in reports 2049, 2063
- Annotation Tool
  - Baseline Monitor Measurement Graphs 396
  - Server-Centric reports 1892
  - settings 2085
- Apache Server monitor 411
- audit log
  - alerts 1941
  - applying templates 1937
  - categories 1943
  - change password 1943
  - configuring 1931
  - create templates 1938
  - delete templates 1938
  - failed login 1942
  - global search and replace operations 1942
  - group operations 1934
  - login and logout 1942
  - modify templates 1938
  - monitor operations 1935
  - overview 1903
  - reports 1941
  - SiteScope startup 1934
  - template alerts 1940
  - template containers 1937
  - template groups 1939
  - template monitors 1940
  - template remote objects 1939
  - template variables 1938
  - update to general Preferences 1935
  - update to other Preferences 1936
- auto template deployment 1643
  - deployment results 1653
  - global variables 1648
  - instance variables 1648
  - limitations 1663
  - mandatory variables 1648

- publishing template changes 1650
- template update report 1652
- troubleshooting 1663
- variables 1648
- XML attributes reference 1426, 1662
- XML elements reference 1660
- XML file example 1646
- XML tag reference 1426, 1660
- XML validator 1650

## B

- BAC Integration Configuration 1907
- BAC integration preferences in SiteScope 1417
- BAC Integration Statistics 1909
- Backup Configuration dialog box 393
- Baseline
  - Activate Baseline dialog box 389
  - activating 314
  - Backup Configuration dialog box 393
  - Calculate Baseline dialog box 383
  - calculating 313
  - error boundary 318
  - Fine-Tune Adherence Levels/Set Boundary dialog box 387
  - good boundary 318
  - how SiteScope calculates the error boundary 321
  - how SiteScope calculates thresholds 320
  - Monitor Measurement Graphs dialog box 394
  - notes and limitations 315
  - Percentile Range Mapping table 381
  - Remove Baseline dialog box 398
  - setting adherence level 317
  - setting monitor thresholds 327
  - Status Report 399
  - threshold values 319
- baseline
  - setting error boundaries 387
- baseline properties 400
- Baseline Settings (Infrastructure Preferences) 1408
- Baseline Settings (monitor properties) 376



- Baseline Status 400
- Best Case Calculation option, in reports 2066
- Best case calculation option, in reports 2055
- BroadVision Application Server monitor 415
- Browsable Windows Performance Counter monitor 419
- browser language preference 1546
- Business Availability Center 152, 1417, 1424
  - changing the Gateway server 154, 1419
  - forwarding SiteScope data 155
- Business Availability Center Preferences 1416
- Business Availability Center-SiteScope connection, using SSL 153, 1418
  
- C**
- Calculate Baseline dialog box 383
- calculating a baseline 313
- Check Point monitor 425
- Choose Changes page, Global Search and Replace 183
- Cisco Works monitor 429
- Citrix monitor 435
- ColdFusion Server monitor 443
- common monitor settings 354
  - Baseline Settings 376
  - Dependencies 360
  - Enable/Disable Associated Alerts 374
  - Enable/Disable Monitor 373
  - General 356
  - HP BAC Integration 370
  - Link Monitor to CI 369
  - Monitor Run 358
  - Search/Filter Tags 375
  - Threshold 362
- Composite monitor 457
- configuration files
  - enabling use of 1377
- configuring BAC integration preferences
  - limitations and troubleshooting 170
- connection methods for UNIX servers 1308
- Content Changes dialog box 1629
- content match
  - examples for log files 279
  - using metacharacters 267
  - using regular expressions 261
  - using string literals 264
  - using system date variables 274
- context menu options
  - diagnostic tools 1878
  - monitor tree 72
  - remote servers tree 83
  - template tree 84
- Copy to Template Tree dialog box 379
- CPU monitor 461
- Credential Preferences
  - concept 1524
  - configuring 1527
  - user interface 1528
- Current Status view 1857
- custom formatting
  - for SiteScope reports 2051, 2065
- custom reports
  - SiteScope Overall Performance 2135
  - System Availability Management reports in 2100
- Custom Settings 1413
- Custom Settings, Infrastructure Preferences 1413
- cygwin OpenSSH, installing on Windows 1328
  
- D**
- daily logs 1955
- Dashboard Filter page 1871
- Dashboard Settings page 1875
- data aggregation 2093
- database alerts
  - working with 1971
- Database Connection tool 198
- Database Counter monitor 467
- Database Information 201
- Database Information tool 201
- Database logging 1449, 1452
- Database Query monitor 477
- DB2 8.x and 9.x monitor 495
- Delete Dashboard Favorites dialog box 1870
- Dependencies Settings 360

## Index

- dependencies, creating 307
- Dependencies, Groups 299
- Dependency dialog box 377
- Deploy Monitors Using the Monitor
  - Deployment Wizard 1821
- deploying a monitor 323
- Deployment Values dialog box 1637
- deprecated monitors 349
- description property, in reports 2046
- detailed monitor information, in reports
  - 2049, 2063
- DHCP Monitor 515
- diagnostic tools 193
  - Processes 228
- diagnostic tools view
  - context menu options 1878
- Diagnostics integration 1421
- Directory monitor 503
- disabling
  - reports 2056
- Disk Space monitor 509
- Display columns, Monitor report 2068
- DNS Lookup tool 203
- DNS Monitor 519

## E

- e-Business Transaction monitor 525
- email
  - integration with 1461, 1462
- Email alerts
  - working with 1973
- email alerts,template properties 1990
- Email Preferences 1461
- e-mail, configuring SiteScope to use 46
- Enable/Disable alerts
  - working with 1972
- Enable/Disable Associated Alerts settings 374
- Enable/Disable Monitor settings 373
- end of report period, for reports 2051
- error boundary, understanding 317
- Error logs 1955
- event log
  - active filters dialog box 2147
- Event Log tool 205
- Event Logs

- viewing 2137
- viewing common event data 2143
- working with event details 2148
- working with event history 2149
- working with reports 2139

Export to file, Monitor report 2069

## F

- F5 Big-IP monitor 533
- Failover
  - integration with 1458
- Failover Preferences 1457
- File format, Monitor report 2069
- File monitor 539
- File name, Monitor report 2069
- filter
  - Dashboard 1871
  - global 106
- Filter Affected Objects dialog box, Global Search and Replace 187
- Filter Monitor Types dialog box 114
- Filter Tags dialog box 116
- Filter Target Servers dialog box 115
- filtering SiteScope objects 105
- filtering tree 106
- filters
  - Event Logs 2139
- format template, for reports 2052
- formatting report options 2051, 2065
- Formula Composite Monitor 547
- FTP Monitor 553
- FTP Server tool 208
  - tools 208
- Full and Partial Monitor Coverage 1818

## G

- General Preferences 1376
  - configuring SiteScope for non-English locale 1547
  - defining Web Script monitor file directory 1378
  - enabling configuration files 1377
  - setting locale data and time settings 1547

- suspending monitors 1377
- viewing UI in a specific language 1549
- General Settings (Groups) 297
- General Settings (Infrastructure Preferences) 1388
- General Settings (monitors) 356
- generate report at property 2056
- generic data integration 1420
- Global Search and Replace 171
  - Override Status Condition 173
  - threshold settings 173
- Global Search and Replace wizard 178
  - Advanced Filter dialog box 187
  - Affected Objects page 186
  - Choose Changes page 183
  - Filter Affected Objects dialog box 187
  - Replace Mode page 181
  - Review Summary page 188
  - Select SiteScope page 179
  - Select Subtype page 181
  - Select Type page 180
  - Summary page 190
- good boundary, understanding 317
- groups 1381
  - configuring SiteScope 297

## H

- Health of SiteScope Server Monitor 1914
  - counters on UNIX 1915
  - counters on Windows 1916, 1917
- help, Quick Help 58
- HP BAC Integration Settings 370
- HP Business Availability Center
  - SiteScope integration with 150
- HP NonStop Event Log monitor 561
- HP NonStop Resources monitor 569
- HP OM Event Monitor 1173
  - configuration files 1174
  - configuring Integration Add-on 1177
  - installing Integration Add-on 1176
  - log files for Integration Add-on 1182
  - overview 1174
  - starting and stopping Integration Add-on 1180
  - support in HP OM cluster 1182

- tuning Integration Add-on 1178
- uninstalling Integration Add-on 1181
- versions supported 1173
- HP OVO Event Monitor 1187
- HP Quality Center
  - monitoring solution 1685
- HP Quality Center Application Server for UNIX 1695
- HP Quality Center Application Server for Windows 1693
- HP Quality Center Solution Template
  - deploying 1689
  - system requirements 1690
- HP Quality Center 9.2/10.0 License Status 1697
- HP QuickTest Professional License Server 1701
- HP Service Manager
  - host monitoring solutions 1703
- HTTPS, accessing primary SiteScope using 1459

## I

- i18N
  - See Internationalization 1545
- ignore errors, in report uptime readings 2048, 2062
- ignore warnings, in report uptime readings 2048, 2062
- include warnings, in report uptime readings 2047, 2061
- Infrastructure Preferences 1387, 1388, 1394, 1405, 1407, 1408, 1413
  - Alert Settings 1403
  - Monitor Settings 1396
- integration
  - generic data 1420
- Integration Monitor logs 1143
- Integration Monitor troubleshooting 1143
- Integration Monitors
  - field mapping 1147
  - field mapping, action directive 1168
  - field mapping, conditional expressions 1168
  - field mapping, event handler

## Index

- structure 1163
  - field mapping, events 1150, 1159
  - field mapping, events example 1155, 1162
  - field mapping, examples 1170
  - field mapping, matching condition 1164
  - field mapping, measurements 1156
  - field mapping, measurements example 1157
  - field mapping, string expressions 1168
  - field mapping, structure 1149
  - field mapping, tags 1169
  - list of deprecated 1142
  - replacing deprecated 1142
  - working with 1129
- Integration preferences
- BAC 1417
  - Business Availability Center 1417
- Internationalization
- multi-lingual user interface support 1546
  - SiteScope limitations 1545
  - SiteScope support 1545
  - SiteScope UNIX supported monitors 1550
  - SiteScope user interface 1545
  - SiteScope Windows supported monitors 1550
- IPMI monitor 573
- J**
- JavaScript in URL sequences 989
  - JBoss Application Server
    - host monitoring solutions 1711
  - JBoss Application Server solution template
    - deploying 1705, 1713
  - JMX console 39
  - JMX monitor 577
- L**
- language preference 1546
  - LDAP Authentication tool 211
  - LDAP monitor 585
  - Link Check monitor 591
  - Link Monitor to CI settings 369
  - Linux Host solution template
    - deploying 1721
  - Linux host, monitoring solution 1719
  - list of errors, in reports 2047, 2061
  - list of goods, in reports 2047, 2061
  - list of warnings, in reports 2047, 2061
  - localization
    - matching local date formats 276
  - Log Event alerts
    - working with 1974
  - Log Event Health Monitor 1910
  - Log File monitor 597
  - Log files
    - data columns 1932
  - log files
    - database table 1450
    - for alerts 1956
    - monitorCount.log 1956
    - of monitor data 1955
    - of operator acknowledgments 1956
    - of post requests 1956
    - preferences 1449, 1452
    - run monitor 1955
    - setting how much data is stored 46
    - silent deployment 1956
    - SiteScope restarts 1955
    - URL monitor details 1956
  - Log Files tab 1954
  - log files, viewing 1903
  - Log Preferences 1449, 1452
  - login, silent 38
  - logs
    - Integration Monitors 1143
- M**
- Mail Monitor 607
  - Mail Round Trip tool 214
  - Manage Monitors and Groups dialog box 68
  - Management report
    - Calculation Method 2055
    - Display Settings 2047
    - Filter and Scheduling Settings 2050

- General Settings 2046
- Management Settings 2056
- Report Distribution 2052
- Report Format 2051
- Report Targets 2046
- Report title 2046
- Management Report dialog box 2045
- management reports
  - working with 2039
- MAPI Monitor 613
- match content
  - using regular expressions 261
- maximum graph value, for reports 2055, 2066
- measurements graph, in reports 2048, 2062
- Memory monitor 623
- Microsoft Exchange
  - monitoring solution 1725
- Microsoft Exchange 2000/2003/2007
  - Message Traffic monitor 655
- Microsoft Exchange 2003 Mailbox monitor 639
- Microsoft Exchange 2003 Public Folder monitor 661
- Microsoft Exchange 2007 monitor 645
- Microsoft Exchange 5.5 Message Traffic monitor 635
- Microsoft Exchange solution template
  - deploying 1728
  - settings 1729
- Microsoft IIS
  - host monitoring solutions 1733
- Microsoft IIS Server monitor 665
- Microsoft IIS solution template
  - deploying 1735
- Microsoft SQL Server
  - host monitoring solutions 1739
- Microsoft SQL Server monitor 671
- Microsoft SQL Server solution template
  - deploying 1741
- Microsoft Windows Dial-up Monitor 679
- Microsoft Windows Event Log monitor 685
- Microsoft Windows Host solution template
  - deploying 1749
- Microsoft Windows Host, monitoring
  - solution 1747
- Microsoft Windows Media Player monitor 693
- Microsoft Windows Media Player tool 218
- Microsoft Windows Media Server monitor 699
- Microsoft Windows Performance Counter monitor 705
- Microsoft Windows Remote Preferences 1276
- Microsoft Windows Resources monitor 713
- Microsoft Windows servers
  - about monitoring remotes 1276
- Microsoft Windows Services State monitor 725
- Microsoft Windows solution template
  - deploying 1755
- Modify Variables page 1631
- monitor
  - baseline thresholds 312
  - categories 303
  - creating dependencies 307
  - creating using templates 1557
  - deployment 323
  - status thresholds 309
- monitor categories list 336
- monitor counter log 1956
- Monitor Deployment Wizard
  - overview 1812
- Monitor Deployment wizard
  - categories 1827
  - template reference 1827
- Monitor Deployment Wizard Concepts and Tasks 1811
- Monitor Deployment Wizard Features and Options 1816
- Monitor Deployment Wizard for Siebel 1820
- monitor filter, in Quick reports 2064
- monitor filter, in reports 2050
- Monitor History view 1866
- Monitor Load Monitor 1913, 1919
- monitor logs 1955
- Monitor Measurement Graphs dialog box 394
- monitor readings, in reports 2048, 2062
- Monitor report
  - example 2076, 2080

## Index

- Monitor Report dialog box 2067
- Monitor reports
  - Display Settings 2068
  - Report Targets 2067
- Monitor Run Settings 358
- Monitor Settings, Infrastructure Preferences 1396
- monitor templates 1557
- monitor tree
  - context menu options 72
  - objects 72
- monitor types 303
  - ports used 344
- monitoring
  - Active Directory 407
  - Apache Server 411
  - BroadVision Application Server 415
  - Browsable Windows Performance Counter 419
  - Check Point firewall server 425
  - Cisco Works 429
  - Citrix 435
  - ColdFusion Server 443
  - Composite 457
  - configuring user permissions on Windows 2000 1283
  - configuring user permissions on Windows XP,2003 1282
  - CPU 461
  - Database Counter 467
  - Database Query 477
  - DB2 8.x and 9.x 495
  - deployment using templates 1557
  - DHCP 515
  - Directory 503
  - Disk Space 509
  - DNS 519
  - e-Business Transaction 525
  - F5 Big-IP 533
  - File 539
  - Formula Composite 547
  - FTP 553
  - HP NonStop Event Log 561
  - HP NonStop Resources 569
  - IPMI 573
  - JMX 577
  - LDAP 585
  - Link Check 591
  - Log File 597
  - Mail 607
  - MAPI 613
  - Memory 623
  - Microsoft Exchange 2000/2003/2007
    - Message Traffic 655
  - Microsoft Exchange 2003 Mailbox 639
  - Microsoft Exchange 2003 Public Folder 661
  - Microsoft Exchange 2007 645
  - Microsoft Exchange 5.5 Message Traffic 635
  - Microsoft IIS Server 665
  - Microsoft SQL Server 671
  - Microsoft Windows Dial-up 679
  - Microsoft Windows Event Log 685
  - Microsoft Windows Media Player 693
  - Microsoft Windows Media Server 699
  - Microsoft Windows Performance Counter 705
  - Microsoft Windows Resources 713
  - Microsoft Windows Services State 725
  - Multi Log 731
  - Network Bandwidth 737
  - News groups 745
  - Oracle 10g Application Server 749
  - Oracle 9i Application Server 753
  - Oracle Database 757
  - Ping 765
  - Port 769
  - Radius server 773
  - Real Media Player 777
  - Real Media Server 781
  - SAP CCMS 787
  - SAP CCMS Alerts 799
  - SAP Java Web Application Server 807
  - SAP Performance 813
  - SAP Work Processes 821
  - Script 833
  - Services 847
  - setting domain privileges 1280
  - Siebel Application Server 855
  - Siebel Log File 867

- Siebel Web Server 873
  - SiteScope server health 1895
  - SNMP 881
  - SNMP by MIB 891
  - SNMP Trap 901
  - Solaris Zone 907
  - SunONE Web Server 917
  - Sybase 923
  - Tuxedo 927
  - UDDI 933
  - UNIX Resources 935
  - URL 941
  - URL Content 959
  - URL List 973
  - URL Sequence 983
  - VMware Performance 1015
  - Web Script Sequence 1025
  - Web Server 1043
  - Web Service 1049
  - WebLogic Application Server 1061
  - WebSphere Application Server 1071
  - WebSphere MQ Status 1103
  - WebSphere Performance 1113
  - XML Metrics 1119
  - monitoring remote servers 306
  - monitoring remote UNIX servers
    - connection methods 1308
    - overview 1276
    - user interface 1299
  - monitoring remote Windows servers 1276
  - monitoring using Secure Shell (SSH) 1317
  - monitors
    - acknowledging events 105
    - common settings 354
    - disabling based on a schedule 1488
    - for .NET 1753
    - for Active Directory 1673
    - for AIX H 1679
    - for HP Quality Center servers 1685
    - for HP Service Manager 1703
    - for JBoss Application Server 1711
    - for Linux host 1719
    - for Microsoft Exchange 1725
    - for Microsoft IIS 1733
    - for Microsoft SQL Server 1739
    - for Microsoft Windows Host 1747
    - for Oracle databases 1759
    - for Siebel servers 1777
    - for Solaris host 1789
    - for WebLogic servers 1795
    - for WebSphere servers 1805
    - ports used in SiteScope 344
    - range schedules for 1489, 1492
    - schedule to run once 1488
    - security, using default authentication
      - credentials 1376
    - supported in Windows environments
      - only 342
    - supporteding WMI 343
    - supporting agentless SSH 1341
    - suspending 1377
    - troubleshooting skipped 1955
  - Multi Log monitor 731
  - multi-lingual user interface support 1546
- N**
- NET
- host monitoring solutions 1753
  - NetScout Event Monitor 1197
    - system requirements 1199
  - Network Bandwidth Monitor 737
  - Network Node Manager
    - forwarding events from 1269
    - writing scripts to export data 1270
  - Network Node Manager Integration
    - about 1269
  - Network Status tool 220
  - New Alert Report dialog box 2070
  - New Management Report dialog box 2045
  - New Monitor page 351
  - New Monitor Report dialog box 2067
  - New Quick Report dialog box 2060
  - new SiteScope page
    - System Availability Management
      - administration 133
  - New View/Edit Filter page 111
  - New/Edit Tag dialog box 116
  - News monitor 745
  - News Server tool 221
- O**

## Index

- OM Event Monitor
  - See HP OM Event Monitor 1173
- OpenSSH for Windows, installing 1335
- Operator log 1956
- Oracle
  - monitoring solution 1759
- Oracle 10g Application Server monitor 749
- Oracle 9i Application Server monitor 753
- Oracle Database monitor 757
- Oracle Database solution template
  - deploying 1762
  - settings 1766
  - template tools for 1762
- OVO Event Monitor
  - See HP OVO Event Monitor 1187

## P

- Page Options
  - Add to Favorites 58
  - Save Layout to User Preferences 58
- pager
  - connectivity with 1473, 1534
- Pager alerts
  - working with 1975
- Pager Preferences 1472
- password
  - changing 1502
  - configuring length, configuring
    - alphanumeric, configuring
    - punctuation 1503
  - configuring requirements 1503
- Percentile Range Mapping Table 381
- Performance Counters tool 223
- permissions
  - SiteScope in System Availability Management 163
- Persistency Settings 1405
- Persistency Settings, Infrastructure Preferences 1405
- Ping Monitor 765
- Ping tool 226
- Port Monitor 769
- ports used for monitoring 344
- Post alerts
  - working with 1976

- Post log 1956
- Preferences
  - Absolute Schedule 1488
  - Business Availability Center 1416
  - Email 1461
  - Failover 1457
  - General 1376
  - Infrastructure 1387
  - Log 1449
  - Pager 1472
  - Range Schedule 1489
  - Search/Filter Tag 1533
  - SNMP Trap 1481
  - User Management 1498
- Prerequisites for Running the Monitor
  - Deployment Wizard 1814
- Processes tool 228
- Publish Results Summary Page 1632
- Publish Template Changes Summary Report 1633
- Publish Template Changes Wizard
  - Content Changes dialog box 1629
  - Modify Variables page 1631
  - Publish Results Summary Page 1632
  - Review Compliance page 1627
  - Select Deployed Groups page 1626
- publishing template changes 1578
  - auto template deployment 1650

## Q

- Quick Help 58
- Quick Report dialog box 2060
- Quick reports
  - Calculation Method 2066
  - Display Settings 2061
  - Export Settings 2069
  - Filter and Scheduling Settings 2064
  - Report Distribution 2065
  - Report Format 2065
  - Report Targets 2060

## R

- Radius monitor 773
- Range Schedule page 1492



- Range Schedule Preferences 1489
- Range Schedules
  - adding 1494, 1495
- Real Media Player monitor 777
- Real Media Player tool 230
- Real Media Server monitor 781
- registering SiteScope 152, 1417, 1424
- Regular Expression tool 232
- regular expressions 261
  - character classes 268
  - defining 263
  - examples for log files 279
  - general date variables 274
  - ignoring character case 272
  - ignoring line breaks 272
  - in template monitors 1574
  - language and country specific date variables 276
  - matching date coded log entries 284
  - matching delimited log file entries 282
  - matching numbers in log files 283
  - matching patterns with metacharacters 267
  - matching punctuation marks 268
  - matching string literals 264
  - metacharacters 267
  - pitfalls in working with 285
  - preserving line breaks 272
  - quantifiers 270
  - retaining match values 273
  - search mode modifiers 271
  - SiteScope date variables 274
  - special substitution for monitor URL or file path 277
  - the \* quantifier 270
  - using alternation 266
- remote servers 1275
  - properties 1288
- remote servers tree
  - context menu options 83
  - objects 83
- remote UNIX server profiles
  - defining 1287
- remote Windows server profiles
  - defining 1280
- Remotes
  - Microsoft Windows remote servers 1276
  - UNIX remote servers 1276
- Remove Baseline dialog box 398
- Replace Mode page, Global Search and Replace 181
- report format, in Quick reports 2065
- report period, Quick reports 2064
- Report Settings 1407
- Report Settings, Infrastructure Preferences 1407
- Report targets
  - Alert report 2046, 2070
  - Alert time period 2071
  - Alert types 2071
  - Detail level 2071
  - Monitor report 2067
  - Quick report 2060
- reports
  - access and permissions 2093
  - amount of data for 2036
  - color coding 2108
  - controlling when reports are generated 2056
  - formatting with templates 2052
  - group performance report 2114
  - HTML format option 2052
  - introduction 2035
  - log files used by 1955
  - logging data to external database 2036
  - New Alert Report dialog box 2070
  - New Management Report dialog box 2045
  - New Monitor Report dialog box 2067
  - New Quick Report dialog box 2060
  - sending by email 2052, 2065
  - sending XML file by email 2054
  - showing monitor thresholds 2047, 2061
  - SiteScope Cross-Performance 2109
    - adding measurements 2112
  - SiteScope Data over Time 2099
  - SiteScope Error Details 2132
  - SiteScope Error Summary 2130

## Index

- SiteScope Group Performance 2099
- SiteScope Monitor Performance 2105
- SiteScope Over Time 2095
- SiteScope Overall Performance 2135
- SiteScope Performance 2099
- SiteScope Status Summary 2122
- SiteScope Uptime Details 2124
- SiteScope Warning Summary 2125
- System Availability Management 2091
- Review Compliancy page 1627
- Review Summary page, Global Search and Replace 188
- Run Monitor log 1955
- S**
- SAP
  - monitoring solution 1769
- SAP CCMS Alerts Monitor
  - user authorization settings 789
- SAP CCMS Alerts monitor 799
- SAP CCMS monitor 787
  - Topology Settings 790
  - troubleshooting and limitations 791
- SAP Java Web Application Server monitor 807
- SAP NetWeaver solution template settings 1773
- SAP Performance monitor 813
- SAP R/3 solution template 1772
  - settings 1773
  - system requirements 1772
- SAP Work Processes monitor 821
  - Topology Settings 824
- Save to Dashboard Favorites dialog box 1869
- schedule
  - Absolute Schedule page 1490
  - Range Schedule page 1492
- schedule filter, in Quick reports 2064
- schedule filter, in reports 2050
- script alerts
  - alert message file 2033
  - passing data to 1979
  - passing data to SiteScope 2032
  - troubleshooting 1980
  - working with 1977
  - writing 2030
- Script Monitor
  - setting a timeout value for script execution 837
- Script monitor 833
- Search/Filter Tag Preferences 1533
- Search/Filter Tags settings 375
- Search/Filter Tags user interface 110
- searching SiteScope objects 105
- secure monitoring with SSH 1318
- security
  - changing user password 1502
  - default login account 45
  - user accounts 1498, 1504
  - using default authentication credentials 1376
- Select Deployed Groups page 1626
- Select SiteScope page, Global Search and Replace 179
- Select Subtype page, Global Search and Replace 181
- Select Type page, Global Search and Replace 180
- Server Settings 1394
- Server Settings, Infrastructure Preferences 1394
- Server Statistics
  - analyzing 1930
  - General page 1944
  - interpreting 1923
  - Perfex Process Pool page 1947
  - Running Monitors page 1945
  - SSH Connections page 1950
  - Telnet Connections page 1952
  - using 1922
- Server Statistics page 95
- Server-Centric Report
  - how to create 1885
- Server-Centric report 1890
  - generating 1881
- Service monitor 847
- Services tool 234
- Show HTML button 1012
- Show parameters, Monitor report 2068
- Show Source button 1012

- Siebel
  - monitoring solution 1777
- Siebel Application Server Monitor
  - setup requirements 857
- Siebel Application Server monitor 855
  - Topology Settings 859
- Siebel Application Server Solution
  - deploying 1780
  - settings 1783
  - system requirements 1781
- Siebel Gateway Server Solution
  - settings 1786
- Siebel Log File monitor 867
- Siebel Web Server monitor 873
  - Topology Settings 875
- Siebel Web Server Solution
  - settings 1787
- silent deployment log 1956
- silent login 38
  - creating a silent login URL 42
- SiteScope
  - accessing administrator account 45
  - and SSH 1318
  - architecture 36
  - auto template deployment 1643
  - configuration data files 1377
  - creating templates 1580
  - key features 35
  - monitor types 303
  - navigating 60
  - scheduling restarts 1378
  - SNMP Preferences 1482
  - solution templates 1665
  - SSH clients 1345
- SiteScope Alert Action 2006
- SiteScope Cross-Performance report 2109
  - adding measurements 2112
  - rescaling 2098
  - scale 2098
- SiteScope cross-performance report
  - creating 2103
- SiteScope Dashboard
  - accessing SiteScope tools 1851
  - Acknowledge dialog box 1867
  - acknowledging monitor status 1850
  - analyze data in SiteScope Dashboard
    - 1851, 1853
    - concepts and tasks 1847, 1881
    - current status view 1857
    - Dashboard filter overview 1849
    - Dashboard Filter page 1871
    - Dashboard Settings page 1875
    - Delete Dashboard Favorites dialog
      - box 1870
    - monitor history view 1866
    - monitor your Windows/UNIX server's
      - resources 1855
    - overview 1848
    - Save to Dashboard Favorites dialog
      - box 1869
    - Server-Centric report 1881, 1890
- SiteScope Dashboard user interface 1856
- SiteScope data
  - forwarding to Business Availability
    - Center 155
- SiteScope Data over Time report 2099
- SiteScope Email Preferences 1462
- SiteScope Error Details report 2132
- SiteScope Error Summary report 2130
- SiteScope Failover Preferences 1458
- SiteScope Group Performance report 2099
- SiteScope groups 297
  - working with 291
- SiteScope Health 1895
  - adding monitors 1903
  - BAC Integration Configuration
    - Monitor 1907
  - BAC Integration Statistics Monitor
    - 1909
  - Health of SiteScope Server Monitor
    - 1914
  - Log Event Health Monitor 1910
  - log events 1901
  - monitor group 1896
  - monitor load 1902
  - Monitor Load Monitor 1913, 1919
  - server health 1902
  - SSL Certificates State monitor 1919
- SiteScope integration
  - HP Business Availability Center with
    - 150
- SiteScope log database table 1450

## Index

- SiteScope Monitor Performance report 2105
- SiteScope monitoring
  - categories 303
  - ports used for 344
  - remote servers 306
  - working with monitors 301
- SiteScope monitoring model 37
- SiteScope monitors
  - monitors without host data 168
- SiteScope Over Time Reports
  - user interface 2104
- SiteScope Over Time reports 2095
- SiteScope Overall Performance report
  - in custom reports 2135
- SiteScope overview 34
- SiteScope Pager Preferences 1473, 1534
- SiteScope Performance report 2099
- SiteScope Preferences 1375
- SiteScope Range Schedule Preferences 1492
- SiteScope Reports 2114
- SiteScope reports 1890, 2035
  - group filters 2139
  - monitor type filters 2139
  - profile filters 2139
  - showing monitor errors 2047, 2061
  - showing monitor good results 2047, 2061
  - showing monitor readings 2048, 2062
  - showing monitor warnings 2047, 2061
  - showing time in error 2049, 2063
  - working with additional filters 2142
- SiteScope restart schedule 1378
- SiteScope Status Summary report 2122
- SiteScope Templates page 1605
- SiteScope Tools menu 97
- SiteScope Uptime Details report 2124
- SiteScope user interface 64
  - common toolbar 58
  - context buttons 59
  - context toolbars 56, 65
  - context tree 57
- SiteScope Warning Details report 2127
- SiteScope Warning Summary report 2125
- SiteScope-Business Availability Center
  - connection, using SSL 153, 1418
- SMS alerts
  - working with 1981
- SNMP
  - configuring SiteScope properties 1481
  - integration with 1481, 1482
- SNMP Browser tool 237
- SNMP by MIB Monitor 891
- SNMP Monitor 881
- SNMP Preferences 1481
- SNMP Recipient Settings 1481
- SNMP tool 241
- SNMP Trap alerts
  - working with 1982
- SNMP Trap Monitor 901
- SNMP trap settings 1481, 1482
- SNMP Trap tool 243
- Solaris Host solution template
  - deploying 1791
- Solaris host, monitoring solution 1789
- Solaris Zones monitor 907
  - Topology Settings 909
  - use-case scenarios 912
- Solution templates
  - Alerts tab 1607
  - overview 1665
  - Properties tab 1671, 2043
  - Select Group dialog box 1636, 1639
- solution templates
  - deploying 1669
  - for Active Directory 1673
  - SAP monitors 1769
  - SiteScope 1665
- solutions sets
  - for .NET 1753
  - for AIX Host 1679
  - for BEA WebLogic 1795
  - for HP Quality Center servers 1685
  - for HP Service Manager 1703
  - for IBM WebSphere 1805
  - for JBoss Application Server 1711
  - for Linux host 1719
  - for Microsoft Exchange 1725
  - for Microsoft IIS 1733
  - for Microsoft SQL Server 1739
  - for Microsoft Windows Host 1747
  - for Oracle database 1759

- for Siebel servers 1777
    - for Solaris host 1789
  - Sort by, Monitor report 2068
  - Sort order, Monitor report 2068
  - sound alerts
    - working with 1983
  - SSH clients
    - external 1348
    - internal Java 1346
    - using SSH version 2 1349
  - SSH monitoring 1317
    - configuration options 1319
    - configuring UNIX servers for 1324
    - configuring Windows servers for 1322
    - cygwin OpenSSH 1323
    - external SSH client 1348
    - installing and configuring SSH server 1326
    - installing Remote NT SSH files 1337
    - internal Java SSH client 1346
    - key based authentication 1352
    - OpenSSH for Windows 1323
    - password authentication for clients 1347
    - SSH client options 1339
    - using SSH2 1349
    - using SSH2 with internal client 1347, 1351
    - version compatibility 1348
    - working with SSH clients 1345
  - SSL
    - Business Availability Center-SiteScope connection 153, 1418
  - SSL Certificates State monitor 1919
  - SSL, accessing SiteScope using 1459
  - Summary page, Global Search and Replace 190
  - SunONE Web Server monitor 917
  - suspending monitor processes 1377
  - Sybase monitor 923
  - Sync SiteScopes wizard 139
  - System Availability Management
    - permissions model 163
  - System Availability Management
    - administration 125
    - new SiteScope page 133
    - overview 120
    - Sync SiteScopes wizard 139
    - troubleshooting 146
  - System Availability Management reports
    - 2091
    - improving report generation times 2094
    - in custom reports 2100
    - overview 2092
    - SiteScope Cross-Performance 2109
      - adding measurements 2112
    - SiteScope Data over Time 2099
    - SiteScope Error Summary 2130
    - SiteScope Group Performance 2099
    - SiteScope Monitor Performance 2105
    - SiteScope Performance 2099
    - SiteScope Status Summary 2122
    - SiteScope Uptime Details 2124
    - SiteScope Warning Summary 2125
    - working with 2093
  - system values
    - accessing in regular expressions 274
- T**
- Technology Database Integration Monitor 1205, 1257
    - setup requirements 1207, 1259
    - step-by-step integration guide 1210
    - troubleshooting 1223, 1261
  - Technology Log File Integration Monitor 1225
    - setup requirements 1227
    - step-by-step integration guide 1228
    - troubleshooting 1240
  - Technology SNMP Trap Integration Monitor 1241
    - about 1242
    - configuring 1243
    - step-by-step integration guide 1243
    - troubleshooting 1253
    - verify SNMP trap reception 1254
  - Technology Web Service Integration Monitor
    - troubleshooting 1267

## Index

- template
  - add regular expression matching 1601
  - auto deployment 1643
  - copying configurations into 1586
  - counter selection examples 1575
  - counter selection using regular expressions 1574
  - creating 1578, 1580
  - examples 1564
  - monitor counter selection in 1573, 1601
  - objects 1562
  - planning 1565
  - publishing changes 1578
  - referencing variables example 1572
  - referencing variables in 1571
  - SERVER\_LIST variable 1569
  - system variables 1569
  - to import or export 1602
  - understanding 1561
  - user-defined variables 1569
  - variables 1567
- Template Settings 1405
- Template Settings, Infrastructure Preferences 1405
- template tree
  - context menu options 84
  - objects 84
- template updates
  - Content Changes dialog box 1629
  - Modify Variables page 1631
  - Publish Results Summary Page 1632
  - Publish Template Changes Summary Report 1633
  - Review Compliancy page 1627
  - Select Deployed Groups page 1626
- Templates
  - Alerts tab 1607
  - Deployment Values dialog box 1637
  - Properties tab 1606, 2043
- templates 1557
  - Export Template dialog box 1623
  - Generate Auto-Deploy XML page 1640
  - Import Template dialog box 1625
  - New Template Alert dialog box 1622
  - New Template Container dialog box 1609
  - New Template dialog box 1611
  - New Template Group dialog box 1617
  - New Template Monitor dialog box 1620
  - New Template Remote dialog box 1615
  - New Template Variable dialog box 1613
  - reserved template groups 1603
  - Select Group dialog box 1636, 1639
  - Select Template dialog box 378
  - updating 1578
- Threshold Settings 362
- thresholds
  - activating a baseline 314
  - availability 310
  - baseline 311
  - calculating a baseline 313
  - multiple 312
  - schedules 310
  - setting 309
  - setting using a baseline 312
  - status impact 311
- Thresholds property, in reports 2047, 2061
- Time Between Samples 2066
- Time between samples 2055
- Time in error, in reports 2049, 2063
- time period for reports 2051
- tools 201
  - Database Connection 198
  - DNS Lookup 203
  - Event Log 205
  - LDAP Authentication 211
  - Mail Round Trip 214
  - Microsoft Windows Media Player 218
  - Network Status 220
  - News Server 221
  - Performance Counters 223
  - Ping 226
  - Real Media Player 230
  - Regular Expression 232
  - Services 234
  - SNMP 241
  - SNMP Browser 237

- SNMP Trap 243
  - TraceRoute 245
  - URL 247
  - Web Service 251
  - XSL Transformation 258
  - toolsplink.exe 1308
  - topology data
    - SiteScope to Business Availability Center 155
  - TraceRoute tool 245
  - troubleshooting
    - a monitored system 193
    - Integration Monitors 1143
    - monitor configuration 193
    - System Availability Management administration 146
  - Tuxedo monitor 927
- U**
- UDDI monitor 933
  - UNIX adaptors
    - adaptor command list 1367
    - adaptor file format 1366
    - adding 1364
    - default adaptor file list 1365
    - working with 1363
  - UNIX Remote servers 1276
    - configuring to monitor on remote server 1285
  - UNIX Resources monitor 935
  - UNIX servers
    - about monitoring remote 1276
    - connection methods 1308
  - uptime and readings options, in reports 2047, 2061
  - URL Content Monitor
    - SSL connectivity 961
  - URL Content monitor 959
  - URL details log 1956
  - URL List monitor 973
  - URL Monitor
    - security, using default authentication credentials 1376
    - SSL connectivity 945, 976
  - URL monitor 941
  - URL Sequence Monitor
    - beginning a new 997
    - copying HTML source in steps 1012
    - defining the next step 998
    - dynamic content 990
    - limitations on embedded scripts 989
    - SSL connectivity 989
    - viewing steps in a browser 1012
  - URL Sequence monitor 983
  - URL Sequence step test 1013
  - URL Sequence Steps dialog box 1007
  - URL tool 247
  - user interface
    - multi-lingual support 1546
  - User Management Preferences 1498
  - user management preferences 1504
  - User Management profiles 1504
  - user profiles 1498, 1504
  - user types 1499
  - Users Preferences
    - changing user password 1502
- V**
- variables
    - in templates 1567
  - VMware Performance monitor 1015
- W**
- Web Script counter metrics 1040
  - Web Script Monitor
    - counters 1028
    - measurements 1028
    - setting up 1028, 1035
    - transaction breakdowns 1028
    - VuGen scripting 1028, 1035
    - workflow 1028, 1035
  - Web Script monitor 1025
  - Web Server monitor 1043
  - Web Service monitor 1049
    - Topology Settings 1053
  - Web Service tool 251
  - WebLogic
    - monitoring solution 1795
  - WebLogic Application Server monitor 1061

## Index

- WebLogic solution template
  - deploying 1798
  - selecting modules to monitor 1799
  - settings 1801
  - using 1799
- WebSphere
  - monitoring solution 1805
- WebSphere Application Server monitor 1071
- WebSphere MQ Status Monitor
  - authentication 1106
- WebSphere MQ Status monitor 1103
- WebSphere Performance monitor 1113
- WebSphere solution template
  - deploying 1807
  - settings 1808
  - system requirements 1807
- Windows Remote servers
  - configuring to monitor on remote server 1277
- Windows servers
  - monitoring remotes 1291
  - perfex for troubleshooting connections 1312
  - troubleshooting event log access 1309
- WMI, monitors supported by 343

## **X**

- XML documents
  - example match content syntax 404
  - monitoring as URLs 404
  - using content match values 406
- XML Metrics monitor 1119
- xml template deployment 1643
- XSL Transformation tool 258