



**Hewlett Packard**  
Enterprise

# HPE SiteScope

Software Version: 11.32

## Monitor Reference

Document Release Date: March 2016  
Software Release Date: March 2016

## Legal Notices

### Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE 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 HPE 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 Notice

© Copyright 2005 - 2016 Hewlett Packard Enterprise Development LP

### 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.

iPod is a trademark of Apple Computer, Inc.

Java is a registered trademark of Oracle and/or its affiliates.

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

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

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:

<https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=>.

This site requires an HPE Passport account. If you do not have one, click the **Create an account** button on the HPE Passport Sign in page.

### Support

Visit the HPE Software Support website at: <https://softwaresupport.hpe.com>

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software 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 website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE 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 HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to <https://softwaresupport.hpe.com> and click **Register**.

To find more information about access levels, go to:

<https://softwaresupport.hpe.com/web/softwaresupport/access-levels>

## HPE Software Integrations and Solutions

Visit the Integrations and Solutions Catalog at <https://softwaresupport.hpe.com/km/KM01702731> to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

# Contents

Welcome to the SiteScope Monitor Reference .....	8
Part 1: SiteScope Monitor Reference Overview .....	9
Chapter 1: SiteScope Monitor Categories .....	10
Chapter 2: Monitor Categories List .....	13
Chapter 3: Monitor Permissions and Credentials .....	18
Chapter 4: Supported Versions and Platforms .....	34
Part 2: SiteScope Monitors (A-Z) .....	49
Chapter 5: Active Directory Replication Monitor .....	50
Chapter 6: Amazon Web Services Monitor .....	53
Chapter 7: Apache Server Monitor .....	57
Chapter 8: BroadVision Application Server Monitor .....	60
Chapter 9: Browsable Windows Performance Counter Monitor .....	64
Chapter 10: Check Point Monitor .....	66
Chapter 11: Cisco Works Monitor .....	68
Chapter 12: Citrix Monitor .....	73
Chapter 13: ColdFusion Server Monitor .....	78
Chapter 14: COM+ Server Monitor .....	82
Chapter 15: Composite Monitor .....	85
Chapter 16: CPU Monitor .....	88
Chapter 17: Custom Monitor .....	92
Chapter 18: Custom Database Monitor .....	105
Chapter 19: Custom Log File Monitor .....	123
Chapter 20: Custom WMI Monitor .....	145
Chapter 21: Database Counter Monitor .....	161
Chapter 22: Database Query Monitor .....	169
Chapter 23: DB2 JDBC Monitor .....	182
Chapter 24: DHCP Monitor .....	188
Chapter 25: Directory Monitor .....	190
Chapter 26: Disk Space Monitor (Deprecated) .....	194
Chapter 27: DNS Monitor .....	198
Chapter 28: Dynamic Disk Space Monitor .....	201
Chapter 28: Dynamic Docker Monitor .....	210
Chapter 29: Dynamic JMX Monitor .....	236
Chapter 30: e-Business Transaction Monitor .....	251
Chapter 31: F5 Big-IP Monitor .....	255
Chapter 32: File Monitor .....	261

Chapter 33: Formula Composite Monitor .....	266
Chapter 34: FTP Monitor .....	270
Chapter 35: Generic Hypervisor Monitor .....	275
Chapter 36: Hadoop Monitor .....	282
Chapter 37: HAProxy Monitor .....	295
Chapter 38: HP iLO (Integrated Lights-Out) Monitor .....	298
Chapter 39: HP NonStop Event Log Monitor .....	302
Chapter 40: HP NonStop Resources Monitor .....	306
Chapter 41: HP Vertica JDBC Monitor .....	310
Chapter 42: IPMI Monitor .....	321
Chapter 43: JMX Monitor .....	323
Chapter 44: KVM Monitor .....	334
Chapter 45: LDAP Monitor .....	343
Chapter 46: Link Check Monitor .....	347
Chapter 47: Log File Monitor .....	350
Chapter 48: Mail Monitor .....	362
Chapter 49: MAPI Monitor .....	366
Chapter 50: Memcached Statistics Monitor .....	371
Chapter 51: Memory Monitor .....	373
Chapter 52: Microsoft ASP Server Monitor .....	378
Chapter 53: Microsoft Exchange Monitor .....	383
Chapter 54: Microsoft Exchange Base Monitor .....	390
Chapter 55: Microsoft Exchange 2000/2003/2007 Message Traffic Monitor .....	408
Chapter 56: Microsoft Exchange 5.5 Message Traffic Monitor (Deprecated) .....	411
Chapter 57: Microsoft Exchange 2003 Mailbox Monitor (Deprecated) .....	413
Chapter 58: Microsoft Exchange 2003 Public Folder Monitor (Deprecated) .....	416
Chapter 59: Microsoft Hyper-V Monitor .....	418
Chapter 60: Microsoft IIS Server Monitor .....	425
Chapter 61: Microsoft Lync Server 2010 Monitors .....	432
Chapter 62: Microsoft SQL Server Monitor .....	446
Chapter 63: Microsoft Windows Dial-up Monitor (Deprecated) .....	453
Chapter 64: Microsoft Windows Event Log Monitor .....	457
Chapter 65: Microsoft Windows Media Player Monitor (Deprecated) .....	466
Chapter 66: Microsoft Windows Media Server Monitor .....	469
Chapter 67: Microsoft Windows Performance Counter Monitor .....	473
Chapter 68: Microsoft Windows Resources Monitor .....	477
Chapter 69: Microsoft Windows Services State Monitor .....	484
Chapter 70: Multi Log Monitor .....	489
Chapter 71: Network Bandwidth Monitor .....	498
Chapter 72: News Monitor .....	503
Chapter 73: Oracle 10g Application Server Monitor .....	506

Chapter 74: Oracle 9i Application Server Monitor .....	513
Chapter 75: Oracle Database Monitor .....	516
Chapter 76: Ping Monitor .....	525
Chapter 77: Port Monitor .....	528
Chapter 78: Radius Monitor .....	531
Chapter 79: Real Media Player Monitor (Deprecated) .....	534
Chapter 80: Real Media Server Monitor .....	536
Chapter 81: REST API Monitor .....	540
Chapter 82: SAP CCMS Monitor .....	547
Chapter 83: SAP CCMS Alerts Monitor .....	553
Chapter 84: SAP Java Web Application Server Monitor .....	557
Chapter 85: SAP MAI Alert Monitor .....	561
Chapter 86: SAP Performance Monitor .....	568
Chapter 87: SAP Work Processes Monitor .....	574
Chapter 88: Script Monitor .....	580
Chapter 89: Service Monitor .....	589
Chapter 90: Siebel Application Server Monitor .....	595
Chapter 91: Siebel Log File Monitor .....	604
Chapter 92: Siebel Web Server Monitor .....	608
Chapter 93: SNMP Monitor .....	615
Chapter 94: SNMP by MIB Monitor .....	622
Chapter 95: SNMP Trap Monitor .....	628
Chapter 96: Solaris Zones Monitor .....	631
Chapter 97: SunONE Web Server Monitor .....	638
Chapter 98: Sybase Monitor (Deprecated) .....	642
Chapter 99: Syslog Monitor .....	645
Chapter 100: Tuxedo Monitor (Deprecated) .....	651
Chapter 101: UDDI Monitor .....	655
Chapter 102: UNIX Resources Monitor .....	656
Chapter 103: URL Monitor .....	661
Chapter 104: URL Content Monitor .....	675
Chapter 105: URL List Monitor .....	688
Chapter 106: URL Sequence Monitor .....	697
Chapter 107: VMware Datastore Monitor .....	720
Chapter 108: VMware Host Monitors .....	731
Chapter 109: VMware Performance Monitor .....	753
Chapter 110: Web Script Monitor .....	770
Chapter 111: Web Server Monitor .....	781
Chapter 112: Web Service Monitor .....	784
Chapter 113: WebLogic Application Server Monitor .....	794
Chapter 114: WebSphere Application Server Monitor .....	800

Chapter 115: WebSphere MQ Status Monitor .....	823
Chapter 116: WebSphere Performance Servlet Monitor .....	832
Chapter 117: XML Metrics Monitor .....	836
<b>Part 3: Integration Monitors (A-Z) .....</b>	<b>840</b>
Chapter 118: HP OM Event Monitor .....	841
Chapter 119: HP Service Manager Monitor .....	851
Chapter 120: NetScout Event Monitor .....	857
Chapter 121: Technology Database Integration Monitor .....	861
Chapter 122: Technology Log File Integration Monitor .....	874
Chapter 123: Technology SNMP Trap Integration Monitor .....	885
Chapter 124: Technology Web Service Integration Monitor .....	895
<b>Send Documentation Feedback .....</b>	<b>909</b>

# Welcome to the SiteScope Monitor Reference

This guide describes how to set up the monitoring environment and configure SiteScope and integration monitors to monitor the enterprise IT infrastructure. It contains information for configuring the specific monitor only. For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## How This Guide Is Organized

This guide covers the following topics:

- ["SiteScope Monitor Reference Overview" on page 9](#)  
Describes the SiteScope monitor classes and category listing formats, the monitors in each monitor category, and the user permissions and credentials needed to access each monitor.
- ["SiteScope Monitors \(A-Z\)" on page 49](#)  
Describes how to set up the monitoring environment and configure each type of SiteScope monitor. It includes information on supported versions, setup requirements, user permissions, and troubleshooting issues.
- ["Integration Monitors \(A-Z\)" on page 840](#)  
Describes how to configure each type of integration monitor, including troubleshooting issues relating to monitoring EMS environments with SiteScope.

**Note:** For details on setting panels in the monitor Properties tab that are common to all monitors, see Common Monitor Settings in Using SiteScope.

## Who Should Read This Guide

This guide is intended for the following users of HPE SiteScope and Business Service Management (BSM):

- SiteScope/BSM administrators
- SiteScope/BSM application administrators
- SiteScope/BSM data collector administrators
- SiteScope/BSM 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 BSM should be familiar with BSM and enterprise monitoring and management concepts.



# Part 1: SiteScope Monitor Reference Overview

# Chapter 1: SiteScope Monitor Categories

SiteScope monitors 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.

**Note:** User permissions and credentials are needed to access each monitor. For details on the required permissions and credentials, and the corresponding protocol used by each monitor, see ["Monitor Permissions and Credentials" on page 18](#).

This section describes the monitor classes and the category listing formats. To see the list of monitors contained in each monitor category, see Monitor Categories List.

## 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 third-party applications. These monitors enable SiteScope to access and retrieve data from the monitored applications.
- **Big Data.** Monitors in this category monitor Big Data platforms to gain real-time visibility and insight into the health and performance of the big data infrastructure.
- **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 different types of environment. These monitors can monitor networks, applications, and databases depending on how they are configured.
- **Media Monitors.** Monitors in this category monitor applications that play media files and stream data.
- **Network Monitors.** Monitors in this category monitor network health and availability.
- **Server Monitors.** Monitors in this category monitor server health and availability.
- **Virtualization and Cloud Monitors.** Monitors in this category monitor virtualized environments and cloud infrastructures.
- **Web Transaction Monitors.** Monitors in this category monitor web-based applications.

## Customizable Monitors

Custom monitors broaden the capabilities of regular SiteScope monitors for tracking the availability and performance of your infrastructure systems and applications. Using custom monitors, you can develop your own solutions for environments that are not supported by predefined SiteScope monitors.

You can create your own monitor that collects data, and define a script that processes the collected data and creates metrics. Each time the custom monitor runs, it updates the metrics and returns a status for the metrics defined in the script.

Custom monitors can be published to the HPE Live Network for sharing with other SiteScope users. For more details on using Custom monitors, see Creating Custom Monitors in the Using SiteScope Guide.

## Dynamic Monitors

Dynamic monitors automatically adjust the SiteScope monitoring configuration based on changes that are happening in your IT environment.

SiteScope provides various dynamic monitors that automatically update themselves over time by adding and removing counters and thresholds as virtual machines move from one host system to another. In addition, baselining is supported, where thresholds are dynamically changed based on historical monitoring data.

Dynamic monitors include:

- Dynamic Disk Space Monitor
- Dynamic Docker Monitor
- Dynamic JMX Monitor
- Generic Hypervisor Monitor
- Hadoop Monitor
- HP Vertica JDBC Monitor
- KVM Monitor
- VMware Datastore Monitor
- VMware Host Monitors

## Integration Monitors

Integration monitors are used to capture and forward data from third-party domain managers or applications (typically Enterprise Management Systems (EMS)) into BSM.

These monitor types require additional licensing and may only be available as part of another HPE product. For more information about Integration Monitor capabilities, see Integration Monitors in the Using SiteScope Guide.

## 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. After deploying solution templates, you can edit or delete them using the same steps as with other monitor types. For more information, see Deploying Solution Templates in the Using SiteScope Guide.

SiteScope provides the following solution templates that include standard SiteScope monitor types and solution-specific monitors:

- Active Directory (with and without Global Catalog)
- AIX Host
- Apache Cassandra
- Apache Tomcat
- Hadoop Cluster Monitoring
- HP Quality Center
- HP QuickTest Professional
- HP Service Manager

- HP Vertica
- JBoss Application Server
- Linux Host (OS )
- Microsoft Exchange
- Microsoft IIS Server
- Microsoft Lync Server
- Microsoft SharePoint
- Microsoft SQL Server
- Microsoft Windows Host
- .NET
- Oracle Database
- SAP Application Server
- Siebel Application/Gateway/Web Server (for UNIX and Windows)
- Solaris Host
- VMware Capacity Management
- VMware Host CPU/Memory/Network/State/Storage
- VMware Host For Performance Troubleshooting
- WebLogic Application Server
- WebSphere Application Server

# Chapter 2: Monitor Categories List

This section displays the SiteScope monitors in each monitor category.

- ["Application Monitors" below](#)
- ["Big Data" on the next page](#)
- ["Customizable Monitors" on the next page](#)
- ["Database Monitors" on the next page](#)
- ["Generic Monitors" on page 15](#)
- ["Integration Monitors" on page 15](#)
- ["Media Monitors" on page 15](#)
- ["Network Monitors" on page 15](#)
- ["Server Monitors" on page 16](#)
- ["Virtualization and Cloud Monitors" on page 16](#)
- ["Web Transaction Monitors" on page 16](#)

## **Application Monitors**

- ["Active Directory Replication Monitor" on page 50](#)
- ["Apache Server Monitor" on page 57](#)
- ["BroadVision Application Server Monitor" on page 60](#)
- ["Check Point Monitor" on page 66](#)
- ["Cisco Works Monitor" on page 68](#)
- ["Citrix Monitor" on page 73](#)
- ["ColdFusion Server Monitor" on page 78](#)
- ["COM+ Server Monitor" on page 82](#)
- ["Dynamic Docker Monitor" on page 210](#)
- ["F5 Big-IP Monitor" on page 255](#)
- ["HAProxy Monitor" on page 295](#)
- ["Mail Monitor" on page 362](#)
- ["MAPI Monitor" on page 366](#)
- ["Memcached Statistics Monitor" on page 371](#)
- ["Microsoft ASP Server Monitor" on page 378](#)
- ["Microsoft Exchange Monitor" on page 383](#)
- ["Microsoft Exchange Base Monitor" on page 390](#)
- ["Microsoft Exchange 2000/2003/2007 Message Traffic Monitor" on page 408](#)
- ["Microsoft Exchange 5.5 Message Traffic Monitor \(Deprecated\)" on page 411](#)
- ["Microsoft Exchange 2003 Mailbox Monitor \(Deprecated\)" on page 413](#)
- ["Microsoft Exchange 2003 Public Folder Monitor \(Deprecated\)" on page 416](#)
- ["Microsoft IIS Server Monitor" on page 425](#)

- "News Monitor" on page 503
- "Oracle 9i Application Server Monitor" on page 513
- "Oracle 10g Application Server Monitor" on page 506
- "Radius Monitor" on page 531
- "SAP CCMS Monitor" on page 547
- "SAP CCMS Alerts Monitor" on page 553
- "SAP Java Web Application Server Monitor" on page 557
- "SAP MAI Alert Monitor" on page 561
- "SAP Performance Monitor" on page 568
- "SAP Work Processes Monitor" on page 574
- "Siebel Application Server Monitor" on page 595
- "Siebel Log File Monitor" on page 604
- "Siebel Web Server Monitor" on page 608
- "SunONE Web Server Monitor" on page 638
- "Tuxedo Monitor (Deprecated)" on page 651
- "UDDI Monitor" on page 655
- "WebLogic Application Server Monitor" on page 794
- "Web Server Monitor" on page 781
- "WebSphere Application Server Monitor" on page 800
- "WebSphere MQ Status Monitor" on page 823
- "WebSphere Performance Servlet Monitor" on page 832

## **Big Data**

- "Hadoop Monitor" on page 282
- "HP Vertica JDBC Monitor" on page 310

## **Customizable Monitors**

- "Custom Monitor" on page 92
- "Custom Database Monitor" on page 105
- "Custom Log File Monitor" on page 123
- "Custom WMI Monitor" on page 145

## **Database Monitors**

- "Database Counter Monitor" on page 161
- "Database Query Monitor" on page 169
- "DB2 JDBC Monitor" on page 182
- "LDAP Monitor" on page 343
- "Microsoft SQL Server Monitor" on page 446
- "Oracle Database Monitor" on page 516
- "Sybase Monitor (Deprecated)" on page 642

## Generic Monitors

- ["Composite Monitor" on page 85](#)
- ["Directory Monitor" on page 190](#)
- ["Dynamic JMX Monitor" on page 236](#)
- ["File Monitor" on page 261](#)
- ["Formula Composite Monitor" on page 266](#)
- ["JMX Monitor" on page 323](#)
- ["Log File Monitor" on page 350](#)
- ["Multi Log Monitor" on page 489](#)
- ["Script Monitor" on page 580](#)
- ["Syslog Monitor" on page 645](#)
- ["Web Service Monitor" on page 784](#)
- ["XML Metrics Monitor" on page 836](#)

## Integration Monitors

- ["HP OM Event Monitor" on page 841](#)
- ["HP Service Manager Monitor" on page 851](#)
- ["NetScout Event Monitor" on page 857](#)
- ["Technology Database Integration Monitor" on page 861](#)
- ["Technology Log File Integration Monitor" on page 874](#)
- ["Technology SNMP Trap Integration Monitor" on page 885](#)
- ["Technology Web Service Integration Monitor" on page 895](#)

## Media Monitors

- ["Microsoft Lync Server 2010 Monitors" on page 432](#) (Microsoft A/V Conferencing Server, Microsoft Archiving Server, Microsoft Director Server, Microsoft Edge Server, Microsoft Front End Server, Microsoft Mediation Server, Microsoft Monitoring and CDR Server, and Microsoft Registrar Server)
- ["Microsoft Windows Media Player Monitor \(Deprecated\)" on page 466](#)
- ["Microsoft Windows Media Server Monitor" on page 469](#)
- ["Real Media Player Monitor \(Deprecated\)" on page 534](#)
- ["Real Media Server Monitor" on page 536](#)

## Network Monitors

- ["DNS Monitor" on page 198](#)
- ["FTP Monitor" on page 270](#)
- ["Microsoft Windows Dial-up Monitor \(Deprecated\)" on page 453](#)
- ["Network Bandwidth Monitor" on page 498](#)
- ["Ping Monitor" on page 525](#)
- ["Port Monitor" on page 528](#)
- ["SNMP Monitor" on page 615](#)

- "SNMP Trap Monitor" on page 628
- "SNMP by MIB Monitor" on page 622

## Server Monitors

- "Browsable Windows Performance Counter Monitor" on page 64
- "CPU Monitor" on page 88
- "Disk Space Monitor (Deprecated)" on page 194
- "DHCP Monitor" on page 188
- "Dynamic Disk Space Monitor" on page 201
- "HP iLO (Integrated Lights-Out) Monitor" on page 298
- "HP NonStop Event Log Monitor" on page 302
- "HP NonStop Resources Monitor" on page 306
- "IPMI Monitor" on page 321
- "Memory Monitor" on page 373
- "Microsoft Windows Event Log Monitor" on page 457
- "Microsoft Windows Performance Counter Monitor" on page 473
- "Microsoft Windows Resources Monitor" on page 477
- "Microsoft Windows Services State Monitor" on page 484
- "Service Monitor" on page 589
- "UNIX Resources Monitor" on page 656

## Virtualization and Cloud Monitors

- "Amazon Web Services Monitor" on page 53
- "Generic Hypervisor Monitor" on page 275
- "KVM Monitor" on page 334
- "Microsoft Hyper-V Monitor" on page 418
- "Solaris Zones Monitor" on page 631
- "VMware Datastore Monitor" on page 720
- "VMware Host Monitors" on page 731 (VMware Host CPU, VMware Host Memory, VMware Host Network, VMware Host State, and VMware Host Storage)
- "VMware Performance Monitor" on page 753

## Web Transaction Monitors

- "e-Business Transaction Monitor" on page 251
- "Link Check Monitor" on page 347
- REST API Monitor
- "URL Monitor" on page 661
- "URL Content Monitor" on page 675
- "URL List Monitor" on page 688
- "URL Sequence Monitor" on page 697



- ["Web Script Monitor" on page 770](#)

# Chapter 3: Monitor Permissions and Credentials

This section contains a table of SiteScope monitors. Each monitor is listed with its corresponding protocol, the user permissions and credentials needed to access the monitor, and any further notes.

The purpose of this section is to provide you with basic information about the permissions needed to secure your SiteScope monitors.

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
Amazon Web Services	HTTPS	AWS AccessKey ID, AWS SecretKey	This monitor uses secret access keys provided by Amazon. User can find them at Amazon's official site under the user's profile. The HTTP connection is secured.
Apache Server	HTTP, HTTPS	None needed unless required to access the server statistics page.	
BroadVision	Proprietary		
CheckPoint Firewall-1	SNMP	Community string.	This monitor does not support SNMP V3, so the community string passes plain text over the network. The target's SNMP agent may be configured so that the community string can only be used to read a subset of the MIB. The implication for such a configuration is that if an unauthorized person obtained the community string, he would only be able to read OIDs from the agent (but not be able to set them).
Cisco Works	SNMP	Community string or user name/password, depending on SNMP version.	<p>The safest possible configuration for this monitor is running it against an agent configured to use SNMP V3 with authentication (SHA or MD5) and DES encryption for privacy. In this configuration, no unencrypted SNMP data passes over the network. This greatly reduces the risk that a malicious user could compromise the monitored device. It does not take into account security vulnerabilities from implementation bugs in the monitored device's SNMP agent.</p> <p>The riskiest configuration of this monitor is to use SNMP V1 with a community string that has both read and write access on the entire MIB implemented by the agent on the monitored device. In this configuration, a malicious user could obtain the community string by eavesdropping on the network, and then use that community string to reconfigure the device.</p>

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
Citrix Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
ColdFusion	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
COM+	HTTP, HTTPS		
CPU (Windows)	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	<p>Add the server where SiteScope is running to the Domain Admin group in Active Directory (for Windows 2003 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.</p> <p>Edit the registry access permissions for all machines in the domain to enable non-admin access. For details on enabling non-admin users to remotely monitor machines with perfmon, see Microsoft Knowledge Base article 164018 (<a href="http://support.microsoft.com/kb/164018/en-us">http://support.microsoft.com/kb/164018/en-us</a>). 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 whose registry has been modified can be monitored without use of a connection profile.</p>
CPU (Solaris/ Linux)	Telnet, SSH, rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permissions to run specific executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.
Database Counter	JDBC	User credentials are needed to authenticate access to the particular database. Each database has a particular method for providing access control to the particular tables that need to be accessed.	The user needs sufficient permission to execute any specified SQL statements.

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
Directory	Shell	Need shell access to the remote server. Supported access protocols are telnet, SSH, and rlogin. It is also necessary for the logged-in user to have permissions to run specific executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.
Directory (Windows)	NetBIOS	Read-only file system access.	Permissions for specific files can be controlled at the operating system level.
Directory (Solaris/ Linux)	Telnet, SSH, rlogin	Read-only file system access to the particular files.	Permissions for specific files can be controlled at the operating system level.
Disk Space (Windows)	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see " <a href="#">Monitoring Performance Objects on Windows</a> " on page 32).	
Disk Space (Solaris/ Linux)	Telnet, SSH, rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permission to run specific executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.
Dynamic Disk Space (Windows)	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see " <a href="#">Monitoring Performance Objects on Windows</a> " on page 32).	
Dynamic Disk Space (Solaris/ Linux)	Telnet, SSH, rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permission to run specific executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.
Dynamic JMX	RMI, IIOP	None needed for SiteScope. The server may require a valid user name and password.	

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
F5 Big-IP	SNMP	Community string or user name/password depending on SNMP version.	<p>The safest possible configuration for this monitor is running it against an agent configured to use SNMP V3 with authentication (SHA or MD5) and DES encryption for privacy. In this configuration, no unencrypted SNMP data passes over the network. This greatly reduces the risk that a malicious user could compromise the monitored device. It does not take into account security vulnerabilities from implementation bugs in the monitored device's SNMP agent.</p> <p>The riskiest configuration of this monitor is to use SNMP V1 with a community string that has both read and write access on the entire MIB implemented by the agent on the monitored device. In this configuration, a malicious user could obtain the community string by eavesdropping on the network, and then use that community string to reconfigure the device.</p>
File (Windows)	NetBIOS, WMI	Windows permissions for read-only access to log file.	
File (Solaris/ Linux)	Telnet, SSH, rlogin	Read-only file permission to the target file system.	
FTP	FTP	Valid user name and password for the FTP site with read-only permission to copy the user-specified file. The customer site may permit anonymous logon.	
Generic Hypervisor	Telnet, SSH, and rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permission to run specific executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.
Hadoop	JMX	Valid user name and password for Hadoop master node JMX.	
HAProxy	HTTP/ HTTPS	None needed for SiteScope. The server may require a valid user name and password.	
HP iLO (Integrated Lights-Out)	SSH	Should be configured by the HP iLO system administrator.	When configuring the remote server, select SSH version 2 only in the Advanced Settings pane (to make it work faster).

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
HP Vertica JDBC	JDBC	Valid user name and password for the Vertica database.	<p>No explicit permissions are required for the following tables; however, users see only the records that correspond to tables they have permissions to view:</p> <ul style="list-style-type: none"> <li>- active_events</li> <li>- disk_storage</li> <li>- configuration_parameters</li> <li>- critical_hosts</li> <li>- critical_nodes</li> <li>- disk_resource_rejection</li> <li>- disk_storage</li> <li>- host_resources</li> <li>- nodes</li> <li>- locks</li> <li>- node_resources</li> <li>- projections</li> <li>- query_metrics</li> <li>- query_profiles</li> <li>- recovery_status</li> <li>- resource_pools</li> <li>- resource_pool_status</li> <li>- resource_queues</li> <li>- resource_rejections</li> <li>- resource_usage</li> <li>- system</li> <li>- system_services</li> <li>- wos_container_storage</li> </ul> <p>The user must be a Superuser to view data from the following tables:</p> <ul style="list-style-type: none"> <li>- database_backups tree branch "Backups"</li> <li>- storage_tiers tree branch "Storage Tiers"</li> <li>- system_resource_usage tree branch "System Resource Usage"</li> </ul>
JMX	RMI, IIOP	None needed for SiteScope. The server may require a valid user name and password.	
KVM	Telnet, SSH, and rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permission to run specific executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
LDAP	LDAP	Valid user name and password on the LDAP server to do simple authentication. Query or search operations require appropriate permissions. Anonymous authentication also supported in version 7.9.	
Link Check	HTTP/HTTPS	None needed unless the HTTP/HTTPS site requires a user name/password.	User needs sufficient permission to click on links.
Log File (Windows)	NetBIOS	Windows permissions for read-only access to log file.	
Log File (Solaris/Linux)	Telnet, SSH, rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permissions to run specific executable programs. Read-only file permissions to the target file system.	It is possible to restrict logged-in users' access by using UNIX group permissions for the command that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.
Mail	SMTP	A valid email account and password.	
MAPI	MAPI	User name/password of one or two email accounts to send and receive test emails.	SiteScope must run as local administrator on the SiteScope server. Test email accounts must have local administrator authority in the SiteScope server.
Memory (Windows)	NetBIOS, WMI	Same as Microsoft ASP Server monitor.	
Memory (Solaris/Linux)	Telnet, SSH, rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permissions to run specific executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.
Memcached Statistics	TCP	None needed.	
Microsoft Archiving Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
Microsoft A/V Conferencing Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft ASP Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft Director Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft Edge Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft Exchange	PowerShell v1.0 (for Microsoft Exchange Server 2007)  PowerShell v2.0 (for Microsoft Exchange Server 2010)	SiteScope must be run by administrator on local machine and this administrator must be in Exchange Server administrators group.	
Microsoft Exchange Base	PowerShell v2	SiteScope must be run by administrator on local machine and this administrator must be in Exchange Server administrators group.	This monitor can monitor: <ul style="list-style-type: none"> <li>• Microsoft Exchange Server 2010 (with SiteScope on an operating system with PowerShell v.2)</li> <li>• Microsoft Exchange Server 2013 (with SiteScope on operating system operating system with PowerShell v.2)</li> </ul>



Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
Microsoft Front End Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft IIS Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft Mediation Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft Monitoring and CDR Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft Registrar Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft SQL Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft Windows Event Log	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
Microsoft Windows Media Player	Telnet, SSH, rlogin	Read-only file permission to the target file system.	
Microsoft Windows Media Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft Windows Performance Counter	NetBIOS	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Microsoft Windows Resources	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Multi Log (Windows)	NetBIOS	Windows permissions for read-only access to log file.	
Multi Log (Solaris/Linux)	Telnet, SSH, rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permissions to run specific executable programs. Read-only file permissions to the target file system.	It is possible to restrict logged-in users' access by using UNIX group permissions for the command that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
Network Bandwidth	SNMP	Community string or user name/password depending on SNMP version.	<p>The safest possible configuration for this monitor is running it against an agent configured to use SNMP V3 with authentication (SHA or MD5) and DES encryption for privacy. In this configuration no unencrypted SNMP data passes over the network. This greatly reduces the risk that a malicious user could compromise the monitored device. It does not take into account security vulnerabilities from implementation bugs in the monitored device's SNMP agent.</p> <p>The riskiest configuration of this monitor is to use SNMP V1 with a community string that has both read and write access on the entire MIB implemented by the agent on the monitored device. In this configuration, a malicious user could obtain the community string by eavesdropping on the network, and then use that community string to reconfigure the device.</p>
News	NNTP	A valid user name and password if the news server requires it, with read-only permission to query total number of messages in the news groups.	
Oracle 9i Application Server	HTTP/HTTPS		
Oracle Database	JDBC	An Oracle user logs in with the ability to execute all the SQL statements found in <b>&lt;SiteScope root directory&gt;\templates.applications\commands.oraclejdbc.</b>	
Ping	ICMP	N/A	
Port	TCP	N/A	
Radius	Radius	A valid user name and password on the Radius server. No other permissions are needed.	SiteScope's IP must be added to the list of servers enabled to communicate with the Radius server. It must also be configured to do PAP authentication.
Real Media Player	Telnet, SSH, rlogin	Read-only file permission on the target file system.	

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
Real Media Server	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
REST API	HTTP/HTTPS	None needed for SiteScope. The server may require a valid user name and password.	
SAP MAI Alert	Proprietary	RFC authorization.	/HPOV/*
SAP CCMS	Proprietary	XMI authorization.	Profiles that have XMI authorization are S_A.SYSTEM, PD_CHICAGO, S_WF_RWTEST, and SAP_ALL.
SAP CCMS Alert	Proprietary		
SAP Performance or SAP Work Processes	Proprietary		
Script (Windows)	Telnet, SSH, rlogin	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .
Script (Solaris/Linux)	Telnet, SSH, rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permissions to run specific executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.
Script on local machine (Solaris, Linux and Windows)	Telnet, SSH, rlogin/NetBIOS	Read-only file permission to the target file system.	
Service (Windows)	NetBIOS, WMI	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on page 32</a> .

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
Service (Solaris/Linux)	Telnet, SSH, rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permissions to run specific executable programs.	It is possible to restrict logged-in users' access by using UNIX group permissions for the commands that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the templates.os files.
Siebel Application Server (previously Siebel Server Manager)	CmdLine	User account must have Siebel Administrator Responsibility privileges to issue Siebel server manager (srvmgr) commands.	If the srvmgr client is remote then a Remote (Windows or UNIX) must be set up with the appropriate user name and password credentials for executing the remote srvmgr command.
Siebel Log	Telnet, SSH, rlogin	File read-only permission to the target Siebel server file system.	
Siebel Web Server	HTTP/HTTPS	User name and password are needed if target Siebel Extensions Page is behind third-party, HTML, form-based authentication software.	User must have permission to retrieve the Siebel SWE page.
SNMP	SNMP	Community string or user name/password, depending on the SNMP version.	<p>The safest possible configuration for this monitor is running it against an agent configured to use SNMP V3 with authentication (SHA or MD5) and DES encryption for privacy. In this configuration, no unencrypted SNMP data passes over the network. This greatly reduces the risk that a malicious user could compromise the monitored device. It does not take into account security vulnerabilities from implementation bugs in the monitored device's SNMP agent.</p> <p>The riskiest configuration of this monitor is to use SNMP V1 with a community string that has both read and write access on the entire MIB implemented by the agent on the monitored device. In this configuration, a malicious user could obtain the community string by eavesdropping on the network, and then use that community string to reconfigure the device.</p>

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
SNMP by MIB	SNMP	Community string or user name and password, depending on the SNMP version.	<p>The safest possible configuration for this monitor is running it against an agent configured to use SNMP V3 with authentication (SHA or MD5) and DES encryption for privacy. In this configuration, no unencrypted SNMP data passes over the network. It greatly reduces the risk that a malicious user could compromise the monitored device. It does not take into account security vulnerabilities from implementation bugs in the monitored device's SNMP agent.</p> <p>The riskiest configuration of this monitor is to use SNMP V1 with a community string that has both read and write access on the entire MIB implemented by the agent on the monitored device. In this configuration, a malicious user could obtain the community string by eavesdropping on the network, and then use that community string to reconfigure the device.</p>
SNMP Trap	SNMP	None, although permissions to configure agents on the network to send traps to SiteScope are required. SiteScope must be running as a privileged user so that it can bind to port 162, a reserved port.	<p>The security risk associated with SNMP V1 and V2 traps is that a malicious user could eavesdrop on the data that is passed in the traps.</p> <p>Using V3 traps with authentication and privacy greatly reduces the chance that data can be used maliciously by eavesdroppers.</p>
SunONE	HTTP/HTTPS	None, unless using a proxy that requires authentication.	
Syslog	Telnet, SSH, rlogin	Need shell access to the remote server. It is also necessary for the logged-in user to have permissions to run specific executable programs. Read-only file permissions to the target file system.	It is possible to restrict logged-in users' access by using UNIX group permissions for the command that SiteScope would run. A list of the relevant commands for a particular operating system can be found in the <b>templates.os</b> files.
Tuxedo	Proprietary	PeopleSoft Tuxedo comes with two preconfigured users, <b>PS</b> and <b>VP</b> , that are monitor-only accounts. No other user can be created or used for SiteScope monitoring.	
URL	HTTP/HTTPS	None needed for SiteScope. The server may require a valid user name and password.	

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
URL Content	HTTP/HTTPS	None needed for SiteScope. The server may require a valid user name and password.	
URL List	HTTP/HTTPS	None needed for SiteScope. The server may require a valid user name and password.	
URL Sequence	HTTP/HTTPS	None needed for SiteScope. The server may require a valid user name and password.	
VMware Datastore	HTTPS	Valid username and password for vCenter	User needs sufficient permissions to view datacenters, datastores, and vmdisks. For vmdisks, user should have Datastore browsable permissions. These monitors also require importing server certificates from vCenter. This can be done using Certificate Management in SiteScope (either before or during monitor configuration, using the Import Certificate option).
VMware Host CPU/ Memory/ Storage/ Network/ State	HTTPS	Valid username and password for vCenter/Host.	User needs sufficient permissions to view hosts and VMs. These monitors also require importing server certificates from vCenter/Host. This can be done manually or by using Certificate Management in SiteScope (either before or during monitor configuration, using the Import Certificate option).
Web Server	NetBIOS	Specific access permissions are required for monitoring performance objects on Windows (see <a href="#">"Monitoring Performance Objects on Windows" on the next page</a> ).	See notes in <a href="#">"Monitoring Performance Objects on Windows" on the next page</a> .
Web Server (Solaris, Linux and Windows)	Telnet, SSH, rlogin	Read-only file permission to the target file system.	
Web Service	HTTP/HTTPS	Supports basic, digest, and NTLM authentication if required by the target Web service.	
WebLogic Application Server 5.x	SNMP	Community string credential must match the string in the SNMP agent.	

Monitor Name	Protocol / Technology	User Permissions and Credentials	Notes
WebLogic Application Server 6.x and later	RMI	Requires a user that belongs to a group with at least monitor role privilege.	
WebSphere Application Server (SOAP over HTTP)	HTTP/ HTTPS	Requires a user that has or belongs to a group with at least the monitor role privilege.	
WebSphere MQ Status	Proprietary	SiteScope account must be a member of mqm group in the MQ Windows server.  In MQ UNIX, the server connection channel used must not require SSL authentication.	
WebSphere Performance Servlet	HTTP/ HTTPS	HTTP authentication through user name and password to the URL of the servlet. Credentials can be customized by the user.	

## Monitoring Performance Objects on Windows

### Access Permissions:

Monitoring performance objects on Windows requires that a user have specific access permissions as described in the Microsoft Knowledge Base for article 300702 (<http://support.microsoft.com/kb/300702/en-us>) and article 164018 (<http://support.microsoft.com/kb/164018/en-us>).

These articles describe the permissions and security policies that should be granted to the user on the monitored server.

### Notes:

- **Perfmon User.** A user that was granted the required privileges to be able to monitor performance objects on Windows servers.

The **Performance Monitor Users** (on Windows 2003), **Power Users**, and **Administrators** groups on Windows servers are already associated with the set of permissions and security policies that are required for a Perfmon User. Any user that belongs to these groups has all required permissions to monitor the performance objects and automatically becomes a Perfmon User. The **Performance Monitor Users** group contains the exact set of privileges whereas the **Power Users** and **Administrators** groups are associated with multiple additional privileges that are not required for performance monitoring.

- **SiteScope User.** The user that the SiteScope service logs on as.

For SiteScope monitors to be able to collect perfmon data from remote servers, connections must be established to these servers using the credentials of a user defined as a Perfmon User. These connections can be established with the following options:



- Configure the SiteScope user to be a domain user that is also a user on the remote machines.
- Where the SiteScope User is not defined as a Perfmon User on remote machines, a Remote NT object must be configured in SiteScope using the credentials of a user that is defined as a Perfmon User on the remote machine. Monitors are then configured to use the Remote NT object.

# Chapter 4: Supported Versions and Platforms

This section contains a table of SiteScope monitors. Each monitor is listed with the versions of the applications and operating systems that are supported for monitoring.

Monitor	Supported Versions and Platforms
Active Directory Replication	This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
Amazon Web Services	This monitor supports monitoring on Amazon CloudWatch API version 2010-08-01.
Apache Server	This monitor supports monitoring remote servers running on Apache 1.3.9, 1.3.12, 2.0, 2.2, 2.4, and 2.4.10 servers.
BroadVision Application Server	This monitor supports monitoring remote servers running on BroadVision 4.1, 5.x, and 6.0 servers.
Cisco Works	This monitor supports monitoring on Cisco Works 2000 servers and later.
Citrix	<ul style="list-style-type: none"><li>• This monitor supports monitoring remote servers running on:<ul style="list-style-type: none"><li>• Citrix MetaFrame 1.8 Service Pack 3</li><li>• Citrix MetaFrame XP(s,a,e) Feature Release 1/Service Pack 1</li><li>• Citrix MetaFrame XP(s,a,e) Feature Release 2/Service Pack 2</li><li>• Citrix Presentation Server 3.5, 4.x</li><li>• Citrix XenApp 4.6, 5.0, 6.0, 6.5, 7.6</li></ul></li><li>• This monitor is supported in SiteScopes running on Windows platforms, and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li><li>• This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li></ul>

Monitor	Supported Versions and Platforms
ColdFusion	<ul style="list-style-type: none"> <li>This monitor supports monitoring ColdFusion 4.5.x, 9, 10, and 11 servers.</li> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see <a href="#">SiteScope Monitoring Using Secure Shell (SSH)</a> in the <a href="#">Using SiteScope Guide</a>.</li> </ul>
COM+ Server	This monitor supports monitoring COM+ software components running on Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2 Update 1.
CPU	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH (for details, see <a href="#">SiteScope Monitoring Using Secure Shell (SSH)</a> in the <a href="#">Using SiteScope Guide</a>).</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see <a href="#">Configure the WMI Service for Remote Monitoring</a> in the <a href="#">Using SiteScope Guide</a>.</li> </ul>
Database Counter	This monitor supports monitoring on any database with a valid JDBC driver that supports SQL queries.
Database Query	This monitor supports monitoring on any database with a valid JDBC driver that supports SQL queries.
DB2 JDBC	<ul style="list-style-type: none"> <li>This monitor supports monitoring DB2 8.x, 9.x, and 10.1 servers.</li> <li>It supports all operating systems with a supported JDBC driver and DB2 snapshot feature.</li> </ul>
Directory	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see <a href="#">SiteScope Monitoring Using Secure Shell (SSH)</a> in the <a href="#">Using SiteScope Guide</a>.</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see <a href="#">"How to Configure the HP NonStop Resources Monitor"</a> on <a href="#">page 307</a>.</li> </ul>

Monitor	Supported Versions and Platforms
Dynamic Disk Space	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see <a href="#">"How to Configure the HP NonStop Resources Monitor" on page 307</a>.</li> <li>This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> </ul>
Dynamic JMX	<p>This monitor supports monitoring on:</p> <ul style="list-style-type: none"> <li>WebLogic 11g (10.3.1-10.3.5), 12c</li> <li>Apache Tomcat 5.0, 5.5, 6.0, 6.0.33, 7.0.25, 7.0.50, 7.0.61, 7.0.62, 8.0.23</li> <li>Oracle Application Server 10.1.3g</li> <li>JBoss servers 4.0.3, 4.2, 5.0, 5.1, 6.0, 6.1, 7.0, 7.1.x</li> <li>JBoss EAP 6.1.x - 6.2.x, 6.3.0</li> <li>Sun Glassfish Enterprise Server 2.1, 3.1</li> <li>WildFly 8.0.0, 8.1.0, 8.2.0</li> </ul>
F5 Big-IP	This monitor supports monitoring F5 Big-IP 4.0, 10.x, 11.x.
File	<ul style="list-style-type: none"> <li>This monitor supports monitoring UNIX remote servers that have been configured in SiteScope and the local SiteScope machine only.</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop monitoring environment, see <a href="#">"How to Configure the HP NonStop Resources Monitor" on page 307</a>.</li> </ul>
Generic Hypervisor	This monitor supports monitoring remote servers running on UNIX remotes only. It has been tested on a KVM environment.
Hadoop	This monitor supports monitoring Hadoop 1.x on GNU/Linux.

Monitor	Supported Versions and Platforms
HAProxy	<p>This monitor supports monitoring HAProxy 1.3, 1.4, and 1.5.10 on remote servers running on:</p> <ul style="list-style-type: none"> <li>Linux 2.4 on x86, x86_64, Alpha, SPARC, MIPS, PARISC</li> <li>Linux 2.6 on x86, x86_64, ARM (ixp425), PPC64</li> <li>Solaris 8/9 on UltraSPARC 2 and 3</li> <li>Solaris 10 on Opteron and UltraSPARC</li> <li>FreeBSD 4.10 - 8 on x86</li> <li>OpenBSD 3.1 to -current on i386, amd64, macppc, alpha, sparc64 and VAX (check the ports)</li> </ul>
HP iLO (Integrated Lights-Out)	The HP iLO monitor supports monitoring HP iLO 2, 3, and 4.
HP NonStop Event Log	<ul style="list-style-type: none"> <li>The minimum officially supported version of the HP NonStop Open System Management (OSM) Event Viewer is T0682 H02 ABU (released May 2009).</li> <li>All G-Series, H-Series, and J-Series NonStop RVUs are supported.</li> </ul>
HP NonStop Resources	All G-Series, H-Series, and J-Series NonStop RVUs are supported.
HP Vertica JDBC	The HP Vertica monitor supports monitoring on Vertica 6.0.1, 6.1, 7.0, 7.1.1.
JMX	<p>This monitor supports monitoring on:</p> <ul style="list-style-type: none"> <li>WebLogic 11g (10.3.1-10.3.5), 12c</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p><b>Note:</b> Monitoring WebLogic 9.x and 10.x is no longer supported due to different Java versions run by SiteScope 11.2x or later, and WebLogic Application Server 9.x and 10.x.</p> </div> <ul style="list-style-type: none"> <li>Apache Tomcat 5.0, 5.5, 6.0, 6.0.33, 7.0.25, 7.0.50, 7.0.61, 7.0.62, 8.0.23</li> <li>Oracle Application Server 10.1.3g</li> <li>JBoss servers 4.0.3, 4.2, 5.0, 5.1, 6.0, 6.1, 7.0, 7.1.x</li> <li>JBoss EAP 6.1.x - 6.2.x, 6.3.0</li> <li>Sun Glassfish Enterprise Server 2.1, 3.1</li> <li>WildFly 8.0.0, 8.1.0, 8.2.0</li> </ul>
KVM	This monitor supports monitoring remote servers running on UNIX remotes only. It has been tested on Linux #29-Ubuntu SMP 3.0.0-16-generic.

Monitor	Supported Versions and Platforms
LDAP	This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
Log File	<ul style="list-style-type: none"> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>This monitor also supports monitoring remote servers running on UNIX and HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see <a href="#">"How to Configure the HP NonStop Resources Monitor" on page 307</a>.</li> </ul>
MAPI	This monitor is supported in SiteScopes that are running on Windows versions only.
Memory	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH (see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide).</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1. <div> <p><b>Note:</b> If you are monitoring a Windows remote server using the NetBIOS method, only virtual memory counters are available.</p> </div> </li> <li>This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide. <div> <p><b>Note:</b> Physical memory (free space and used %) can only be monitored on Windows remote servers using the WMI connection method.</p> </div> </li> <li>Monitoring physical and virtual memory is not supported using the Rlogin connection method on UNIX remote servers.</li> </ul>

Monitor	Supported Versions and Platforms
Microsoft ASP Server	<ul style="list-style-type: none"> <li>• This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>• This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>• This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> </ul>
Microsoft Exchange	This monitor supports monitoring Microsoft Exchange Server 2007 with PowerShell v1.0, and Microsoft Exchange Server 2010 with PowerShell v2.0.
Microsoft Exchange Base	<p>Microsoft Exchange Server 2010 and 2013 on Windows platforms only.</p> <p><b>Note:</b> PowerShell v2.0 must be used on the SiteScope-side.</p>
Microsoft Exchange 2003 Mailbox (Deprecated)	This monitor is supported in SiteScopes that are running on Windows versions only.
Microsoft Exchange 2000*/2003*/2007 Message Traffic (*Deprecated)	This monitor is supported in SiteScopes that are running on Windows versions only.
Microsoft Exchange 2003 Public Folder (Deprecated)	This monitor is supported in SiteScopes that are running on Windows versions only.

Monitor	Supported Versions and Platforms
Microsoft Hyper-V	<ul style="list-style-type: none"> <li>• This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>• This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1. All these supported operating systems should be with Hyper-V role enabled.</li> <li>• This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> </ul>
Microsoft IIS Server	<ul style="list-style-type: none"> <li>• This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>• The Microsoft IIS Server monitor supports monitoring the following: <ul style="list-style-type: none"> <li>• HTTP/HTTPS services on IIS 4.0, 5.0, 7.0, 7.5, 8.0, 8.5.</li> <li>• HTTP/HTTPS, FTP, NNTP and MSMQ Queue on IIS 6, 7.0, 8.0, 8.5.</li> </ul> </li> <li>• This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>• This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> </ul>
Microsoft Lync Server 2010	<ul style="list-style-type: none"> <li>• This monitor supports monitoring Microsoft Lync Server 2010 servers.</li> <li>• This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>• This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> </ul>



Monitor	Supported Versions and Platforms
Microsoft SQL Server	<ul style="list-style-type: none"> <li>• The Microsoft SQL Server monitor supports monitoring Microsoft SQL Server versions 6.5, 7.1, 2000, 2005, 2008, 2008 R2, 2012, and 2014.</li> <li>• This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>• This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012.</li> <li>• This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> </ul>
Microsoft Windows Dial-up (Deprecated)	<ul style="list-style-type: none"> <li>• This monitor is supported in SiteScopes that are running on Windows versions only.</li> <li>• This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012.</li> </ul>
Microsoft Windows Event Log	<ul style="list-style-type: none"> <li>• This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>• This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>• This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> </ul>
Microsoft Windows Media Player (Deprecated)	<ul style="list-style-type: none"> <li>• This monitor is supported in SiteScopes that are running on Windows versions only.</li> <li>• This monitor supports monitoring Windows Media Player 7.x, 9.x, 10.x, 11.0, and 12.</li> <li>• Monitor video streams only with this monitor (not audio streams).</li> <li>• This monitor does not support the .asx or .mov formats.</li> </ul>

Monitor	Supported Versions and Platforms
Microsoft Windows Media Server	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>This monitor supports all supported versions of Microsoft Windows Media Server through perfmon. <b>Note:</b> Windows Media Server is supported and maintained by Microsoft up to and including Windows Server 2008 R2 only.</li> <li>This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> </ul>
Microsoft Windows Performance Counter	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> </ul>
Microsoft Windows Resources	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> </ul>
Microsoft Windows Services State	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> </ul>

Monitor	Supported Versions and Platforms
Multi Log	<ul style="list-style-type: none"> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>This monitor also supports monitoring remote servers running on UNIX and HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see <a href="#">"How to Configure the HP NonStop Resources Monitor" on page 307</a>.</li> </ul>
Network Bandwidth	This monitor supports monitoring remote SNMP-enabled network appliances.
Oracle 10g Application Server	This monitor supports monitoring Oracle 10g and 10g R3 application servers.
Oracle 9i Application Server	This monitor supports monitoring Oracle 9i application servers.
Oracle Database	The monitor supports monitoring server performance statistics from Oracle Database 8i, 9i, 10g, 11i, 11g R2 (11.2.0.1), 11g R2 Real Application Clusters (RAC), and 12c (12.1.0.1) servers.
Real Media Player (Deprecated)	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes that are running on Windows versions only.</li> <li>This monitor supports monitoring RealNetworks Real Media Player versions 7.x, 8.x, 9.x, and 10.x</li> <li>This monitor does not support metadata files such as the .smi format.</li> </ul>
Real Media Server	This monitor is supported in SiteScopes running on Windows platforms, and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
SAP CCMS	This monitor supports monitoring 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.
SAP CCMS Alerts	This monitor enables supports monitoring 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.
SAP Java Web Application Server	<p>This monitor supports monitoring:</p> <ul style="list-style-type: none"> <li>SAP Java Web Application Server 6.40, 7.00, 7.01, 7.02, 7.3</li> <li>SAP Enterprise Portal 5.0, 6.0</li> <li>SAP NetWeaver Portal 7.0, 7.3</li> </ul>

Monitor	Supported Versions and Platforms
SAP MAI Alerts	This monitor supports monitoring on SAP Solution Manager 7.1.
SAP Performance	This monitor supports monitoring SAP Application Servers R/3 4.6B, R/3 4.6C, R/3 4.7E, SAP ECC5 and SAP ECC6.
SAP Work Processes	This monitor supports monitoring SAP Application Servers R/3 4.6B, R/3 4.6C, R/3 4.7E, SAP ECC5 and SAP ECC6.
Script	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>The Script monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see <a href="#">"How to Configure the HP NonStop Resources Monitor" on page 307</a>.</li> </ul>
Service	<ul style="list-style-type: none"> <li>This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.</li> <li>This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> </ul>
Siebel Application Server	This 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, 8.0, 8.1, 8.2 - 8.2.2.4 application servers.
Siebel Log File	This monitor supports monitoring remote servers running on Siebel Application Server 7.03, 7.04, 7.5.3, 7.7, 8.0, 8.1, 8.2 - 8.2.2.4.
Siebel Web Server	This monitor supports monitoring remote servers running on Siebel Application Server 7.03, 7.04, 7.5.3, 7.7, 8.0, 8.1, 8.2 - 8.2.2.4.
SNMP	<ul style="list-style-type: none"> <li>This monitor supports monitoring agents of SNMP versions 1.0, 2.0, and 3.0 MD5 and SHA.</li> <li>This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012.</li> </ul>

Monitor	Supported Versions and Platforms
SNMP by MIB	<ul style="list-style-type: none"> <li>• This monitor supports monitoring agents of SNMP versions 1, 2, and 3 MD5.</li> <li>• This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012.</li> </ul>
SNMP Trap	The monitor supports monitoring traps of SNMP versions 1, 2, and 3.
Solaris Zones	This monitor supports monitoring machines that are running on the following Solaris operating systems: Solaris 10 update 7 (5/09) - Solaris 10 update 11 (01/13), Solaris 11.2.
SunONE Web Server	This monitor supports monitoring SunONE or iPlanet 6.x or 7.0 servers.
Sybase	<ul style="list-style-type: none"> <li>• This monitor supports monitoring the server performance data for Sybase 11.0, 11.5, 11.92, 12.x, and 15.5 database servers.</li> <li>• This monitor is supported in SiteScopes that are running on Windows versions only.</li> <li>• This monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.</li> </ul>
Tuxedo	<ul style="list-style-type: none"> <li>• This monitor supports monitoring server performance data for Oracle Tuxedo 6.5, 7.1, 8.0, 8.1, 9.0, and 9.1 servers.</li> <li>• 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.</li> <li>• This monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.</li> </ul>
UDDI	This monitor supports monitoring of the UDDI 2.0 server.

Monitor	Supported Versions and Platforms
UNIX Resources	<p>This monitor supports monitoring UNIX remote servers running on:</p> <ul style="list-style-type: none"> <li>• Solaris 2.7, 2.8, 2.9, 5.10, 7, 8, 9, 10, 10 8/11 ("U10"), 10 1/13 ("U11"), 11, 11.2</li> <li>• Red Hat Linux 7.x, 8.x, 9.x</li> <li>• Red Hat Linux AS/ES Linux 3.x, 4.x, 5.2, 5.4 - 5.10, 6.0 - 6.5, 7</li> <li>• Oracle Enterprise Linux 6.4, 6.5, 7.0</li> <li>• HP-UX 11iv1 (B.11.11) on HP 9000 series: <ul style="list-style-type: none"> <li>• HP-UX B.11.11 U 9000/800 4030070275 unlimited-user license</li> <li>• HP-UX B.11.31 U ia64 4005705783 unlimited-user license</li> <li>• HP-UX 11i v3</li> </ul> </li> <li>• AIX 5.2, 5.3, 6.1, 7.0, 7.1</li> </ul> <p><b>Note:</b> The UNIX Resources monitor does not support monitoring remote servers running on HP NonStop operating systems; use the <a href="#">"HP NonStop Resources Monitor" on page 306</a> instead.</p>
URL	The URL monitor supports monitoring HTTP versions 1.0 and 1.1.
URL Content	The URL Content monitor supports monitoring HTTP versions 1.0 and 1.1.
URL List	The URL List monitor supports monitoring HTTP versions 1.0 and 1.1.
VMware Datastore	This monitor supports monitoring remote servers running on VMware vSphere 4.0, 4.1, 5.0, 5.1, 5.5, 6.0.
VMware Host	<p>This monitor supports monitoring remote servers running on:</p> <ul style="list-style-type: none"> <li>• VMware VirtualCenter 2.x</li> <li>• VMware ESX 3.x, 4.0, 4.1</li> <li>• VMware ESXi 3.5, 4.0, 4.1, 5.0, 5.1, 5.5, 6.0</li> <li>• VMware ESX 2.5 via VirtualCenter 2.x</li> <li>• VMware ESX 3.x via VirtualCenter 3.x</li> <li>• VMware vSphere 4.0, 4.1, 5.0, 5.1 (also supported with SSO login), 5.5, 6.0</li> </ul> <p><b>Note:</b> Monitoring VMware ESX(i) is not supported when Lockdown mode is enabled.</p>

Monitor	Supported Versions and Platforms
VMware Performance	<p>This monitor supports monitoring remote servers running on:</p> <ul style="list-style-type: none"> <li>• VMware VirtualCenter 2.x</li> <li>• VMware ESX 3.x, 4.0, 4.1</li> <li>• VMware ESXi 3.5, 4.0, 4.1, 5.0, 5.1, 5.5, 6.0</li> <li>• VMware ESX 2.5 via VirtualCenter 2.x</li> <li>• VMware ESX 3.x via VirtualCenter 3.x</li> <li>• VMware vSphere 4.0, 4.1, 5.0, 5.1 (also supported with SSO login), 5.5, 6.0</li> </ul> <p><b>Note:</b> Monitoring VMware ESX(i) is not supported when Lockdown mode is enabled.</p>
Web Script	<ul style="list-style-type: none"> <li>• This monitor is supported in SiteScopes running on Windows and Linux 64-bit environments (SiteScope is no longer supported on 32-bit operating systems).</li> <li>• This monitor supports scripts created in VuGen version 12.02 (scripts created in VuGen versions 9.51 and earlier are retained for backward compatibility).</li> <li>• From SiteScope 11.30 onwards: To use the Web Script monitor, you must install HP Load Generator 12.02 on the SiteScope server to run web scripts.</li> </ul> <p>For details on downloading VuGen 12.02 and HP Load Generator 12.02, see <a href="#">"How to Configure the Web Script Monitor" on page 776</a>.</p>

Monitor	Supported Versions and Platforms
Web Service	<p>The following specification features are currently supported:</p> <ul style="list-style-type: none"> <li>• WSDL 1.1, 2.0</li> <li>• SOAP 1.1, 1.2</li> <li>• Simple and Complex Types based on XML Schema 2001</li> <li>• SOAP binding with the HTTP(S) protocol only</li> <li>• SOAP with Attachments is not supported</li> <li>• Nested WSDL</li> <li>• WSDL with multi-ports and multi-services</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• WSS (Web Services Security) is currently 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. 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: <pre>parameters[COMPLEX] =&lt;pPatientSSN xsi:type="xs:string"&gt;***&lt;/pPatientSSN&gt;</pre> you can modify it by deleting the <b>xs:</b> and <b>xsi:</b> as follows: <pre>parameters[COMPLEX] =&lt;pPatientSSN type="string"&gt;***&lt;/pPatientSSN&gt;</pre> </li> </ul>
WebLogic Application Server	This monitor supports monitoring WebLogic Application Servers version 6 through 8. To monitor a WebLogic Application Server 11g (10.3.1-10.3.5) or 12c, use a JMX monitor.
WebSphere Application Server	This monitor supports monitoring server performance statistics from WebSphere 5.x, 6.0x, 6.1x, 7.0x, 8.0x, and 8.5x servers.
WebSphere MQ Status	<ul style="list-style-type: none"> <li>• This monitor supports monitoring on WebSphere MQ (formerly known as MQSeries) Servers 5.2, 5.3, 5.3.1, 6.0, 7.0, 7.0.1, 7.0.1.3, 7.1, 7.1.0.5, 7.5, 8.0, 8.0.0.2, and 8.0.0.4.</li> <li>• This monitor is indifferent to the platform on which the WebSphere MQ server is installed, whether it is Windows, z/OS, HP-UX, Linux, AIX, or Sun Solaris.</li> </ul>
WebSphere Performance Servlet	This monitor supports monitoring 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, 7.0, 7.0.0.19, 7.0.0.21, 8.0, 8.0.0.1, and 8.0.0.2 servers.



## Part 2: SiteScope Monitors (A-Z)

# Chapter 5: Active Directory Replication Monitor

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.

## To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click the **Active Directory** solution template that you require, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

## Learn About

This section includes:

- ["Active Directory Replication Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["License Consumption" below](#)

### Active Directory Replication Monitor Overview

The Active Directory Replication monitor 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. The error and warning thresholds for the monitor can be set on each of the monitored Domain Controllers.

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.

### Supported Platforms/Versions

This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.

### License Consumption

Points-based Usage	Capacity-based Usage
Active Directory with Global Catalog - 34 points	Requires Active Directory Solution Template. Not available with Community edition.
Active Directory with no Global Catalog - 33 points	
License point usage is based on the solution template cost.	

# Tasks

## How to Configure the Active Directory Replication Monitor

### 1. Prerequisites

- This monitor is only displayed in the user interface after deploying an Active Directory solution template. To enable the monitor, you must have an Operating System Instance (OSi) license with sufficient available capacity. For license purchase inquiries (or if you require additional capacity), contact your HPE sales representative or use the “Contact Us” link in the [HPE SiteScope Product page](#).
- The **LDAP Authentication Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see LDAP Authentication Status Tool in the Using SiteScope Guide.

### 2. Deploy the Active Directory Solution template

For details on using templates to deploy monitors, see SiteScope Templates in the Using SiteScope Guide.

For details on the Active Directory solution template, see Active Directory Solution Templates in the Using SiteScope Guide.

### 3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors.

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Active Directory Replication Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Domain controller</b>	Domain controller that contains the replicated data.
<b>Replicating domain controllers</b>	Comma separated list of domain controllers that replicate data from the domain controller entered above.

UI Element	Description
User name	<p>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>
Password	<p>Password for the Domain Admin account.</p>
Maximum replication time (seconds)	<p>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>
Polling interval (seconds)	<p>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>
Directory path	<p>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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Chapter 6: Amazon Web Services Monitor

The Amazon Web Services monitor enables monitoring of Amazon Web Services (AWS) cloud resources.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Amazon Web Services monitor.

## Learn About

This section includes:

- ["Amazon Web Services Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["License Consumption" below](#)

### Amazon Web Services Monitor Overview

The Amazon Web Services monitor enables monitoring of Amazon Web Services (AWS) cloud resources, starting with Amazon Elastic Compute Cloud service (EC2) and Amazon Virtual Private Cloud (VPC). It provides data on resource utilization, operational performance, and overall network demand patterns.

Data collected from AWS-hosted applications can also be reported to Amazon CloudWatch using the Amazon CloudWatch integration. This data can then be used for AWS AutoScaling, reporting and alerting. For details on enabling the Amazon CloudWatch integration, see Amazon CloudWatch Integration Preferences.

### Supported Platforms/Versions

This monitor supports monitoring on Amazon CloudWatch API version 2010-08-01.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	This monitor does not consume any OS instances, URL or Transaction licenses. Note: This monitor is not available when using Community edition.

## Tasks

### How to Configure the Amazon Web Services Monitor

#### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.

- This monitor is available with all editions except Community edition. Contact your HPE sales representative for more information.
  - The Amazon CloudWatch Service is required to monitor Amazon Web Services.
2. Configure the monitor properties  
Configure the monitor properties as required.  
For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Amazon Web Services Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>AWS Access Key ID</b>	An alphanumeric token that uniquely identifies a request sender. This ID is associated with your AWS Secret Access Key.
<b>AWS Secret Key</b>	The key assigned to you by AWS when you sign up for an AWS account. Used for request authentication.
<b>Socket timeout (milliseconds)</b>	<p>Amount of time, in milliseconds, to 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. A value of zero means there is no timeout used.</p> <p><b>Default value:</b> 120 milliseconds</p>
<b>Region</b>	<p>The Amazon EC2 region that is used to get or store measurements.</p> <p><b>Default value:</b> US East (Northern Virginia)</p> <p><b>Note:</b> When configuring the monitor in template mode, enter the Amazon region ID in the <b>Region ID</b> box as follows:</p> <ul style="list-style-type: none"><li>• <b>us-east-1</b> for US East (Northern Virginia)</li><li>• <b>us-west-2</b> for US West (Oregon)</li><li>• <b>us-west-1</b> for US West (Northern California)</li><li>• <b>eu-west-1</b> for EU (Ireland)</li><li>• <b>ap-southeast-1</b> for Asia Pacific (Singapore)</li><li>• <b>ap-southeast-2</b> for Asia Pacific (Sydney)</li><li>• <b>ap-northeast-1</b> for Asia Pacific (Tokyo)</li><li>• <b>sa-east-1</b> for South America (Sao Paulo)</li><li>• <b>us-gov-west-1</b> for AWS GovCloud</li></ul>

UI Element	Description
<b>Get Regions</b>	<p>Opens the Get Regions dialog box, enabling you to select the Amazon EC2 region that is used to get or store measurements. Amazon EC2 is currently available in the following regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), South America (Sao Paulo), and AWS GovCloud.</p> <p><b>Note:</b> This button is not available when configuring the monitor in template mode; you must manually enter the region ID using one of the IDs listed in <b>Region</b> above.</p>
<b>Counter Settings</b>	
<b>Counters</b>	Server performance counters to check with this monitor. The list displays the available counters and those currently selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see " <a href="#">Monitor Counters</a> " below.
<b>Proxy Settings</b>	
<b>NTLM V2 Proxy</b>	Select if the proxy requires authentication using NTLM version 2.
<b>Address</b>	Domain name and port of an HTTP Proxy Server if a proxy server can be used to access the AWS cloud resources to be monitored.
<b>User name</b>	<p>Proxy server user name if required to access the AWS cloud resources.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Password</b>	<p>Proxy server password if required to access the AWS cloud resources.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authentication for these options to function.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

The Amazon Web Services monitor provides the ability to get statistics for all available metrics stored for the AWS account owner which you can see in the Amazon CloudWatch Management Console. It might be metrics from different Amazon services such as EC2, billing, or your own custom metrics (for example, metrics which SiteScope can send to Amazon using Amazon integration).

If you want to monitor Amazon EC2 instances, you can select the AWS/EC2 group of counters. Below is the list of counters that can be configured for EC2 instances:

- CPUUtilization
- NetworkIn
- NetworkOut

- DiskWriteOps
- DiskReadBytes
- DiskReadOps
- DiskWriteBytes
- StatusCheckFailed
- StatusCheckFailed\_Instance
- StatusCheckFailed\_System

## Tips/Troubleshooting

### General Tips/Limitations

- The Amazon Web Services monitor does not get counters from isolated regions such as AWS GovCloud and China.

**Workaround:** Create the Amazon Web Services monitor using a template, and set the region Id. Make changes to this monitor through the template only, and publish the changes using the Publish Template Changes Wizard.

- The Amazon Web Services Monitor gets data from instances that have detailed monitoring enabled in the AWS Management Console. It can also get data from instances with basic monitoring enabled, but you must add the **\_amazonCloudWebServiceMonitorPeriod** key with a value in minutes to the **<SiteScope root directory>\groups\master.config** file (it is recommended to set value to =10 or greater).

Note that detailed monitoring aggregates metrics data by image ID, instance ID, instance type, and so forth, while basic monitoring aggregates metrics data by Instance ID only.

- Amazon does not store data sent from SiteScope via the Amazon integration or from Amazon instances for more than two weeks (old data is automatically removed). As a result, the Amazon Web Services monitor does not return data older than two weeks.
- By default, SiteScope gets data from AWS-hosted applications at a 2-minutes interval. You can customize the period for receiving data from Amazon by adding the **\_amazonCloudWebServiceMonitorPeriod** property (and a value in minutes) to the **<SiteScope root directory>\groups\master.config** file. For example, **\_amazonCloudWebServiceMonitorPeriod=10** means that SiteScope gets the average values of metrics for the last 10 minutes.
- Deploying an Amazon Web Services monitor in a template might cause SiteScope to crash if the template is deployed against an environment with a large number of counters available.

**Workaround:**

- (1) Add the **\_browsableCountersFilter** property to the **<SiteScope root directory>\groups\master.config** file, and include any comma-separated strings that can be found in the required counter names. For example, Custom dimensions,By LoadBalancer Name.
- (2). Restart SiteScope.



# Chapter 7: Apache Server Monitor

Use the Apache Server monitor to monitor the content of server administration pages for Apache 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Apache Server monitor.

## Learn About

### Supported Platforms/Versions

This monitor supports monitoring remote servers running on Apache 1.3.9, 1.3.12, 2.0, 2.2, 2.4, and 2.4.10 servers.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

## Tasks

### How to Configure the Apache Server Monitor

#### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- 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](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.

2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Apache Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server Settings</b>	
<b>Administration URL</b>	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>	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>	
<b>Counters</b>	Server performance counters to check with this monitor. The list displays the available counters and those currently selected for this monitor.  For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a> .
<b>Connection Settings</b>	
<b>Authorization user name</b>	User name if the server you want to monitor requires a name and password for access.
<b>Authorization password</b>	Password if the server you want to monitor requires a name and password for access.
<b>HTTP Proxy</b>	Domain name and port of an HTTP Proxy Server if required by the proxy server is to access the server.
<b>Proxy user name</b>	Proxy server user name if required to access the server. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy password</b>	Proxy server password if required to access the server. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.

UI Element	Description
<b>Timeout (seconds)</b>	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

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<b>Counters for server-status?auto</b> <ul style="list-style-type: none"><li>• Total Accesses</li><li>• Total kBytes</li><li>• CPUload</li><li>• Uptime</li><li>• ReqPerSec</li><li>• BytesPerSec</li><li>• BytesPerReq</li><li>• BusyWorkers</li><li>• IdleWorkers</li></ul>	<b>Counters for server-status?refresh=30</b> <ul style="list-style-type: none"><li>• Server Version</li><li>• Server Built</li><li>• Current Time</li><li>• Restart Time</li><li>• Parent Server Generation</li><li>• Server uptime</li><li>• Total accesses</li><li>• Total Traffic</li><li>• CPU Usage</li><li>• CPU load</li><li>• requests/sec</li><li>• B/second</li><li>• B/request</li><li>• requests currently being processed</li><li>• idle workers</li></ul>
---	---

# Chapter 8: BroadVision Application Server Monitor

Use the BroadVision Application Server monitor to monitor the server performance data for BroadVision 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. The error and warning thresholds for the monitor can be set on one or more BroadVision server performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the BroadVision Application monitor.

## Learn About

### Supported Platforms/Versions

This monitor supports monitoring remote servers running on BroadVision 4.1, 5.x, and 6.0 servers.

### License Consumption

Points-based Usage	Capacity-based License
One point per metric	One OSI license per monitored host

## Tasks

### How to Configure the BroadVision Application Server Monitor

1. Prerequisites
  - Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
  - 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.
2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### BroadVision Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>Server</b>	BroadVision root server name of the BroadVision server you want to monitor. For example, 199.123.45.678.
<b>Port</b>	ORB port number to the BroadVision server you want to monitor. <b>Example:</b> 1221
<b>Counter Settings</b>	
<b>Counters</b>	Server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a> .  <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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<b>BV_SRV_CTRL</b> <ul style="list-style-type: none"> <li>• BVLOG</li> <li>• SHUTDOWN</li> </ul> <b>BV_SRV_STAT</b> <ul style="list-style-type: none"> <li>• CPU</li> <li>• IDL</li> <li>• LWP</li> <li>• RSS</li> <li>• STIME</li> <li>• SYS</li> <li>• USR</li> <li>• VSZ</li> </ul> <b>NS_STAT</b> <ul style="list-style-type: none"> <li>• BIND</li> <li>• LIST</li> <li>• NEW</li> <li>• REBND</li> <li>• RSOLV</li> <li>• UNBND</li> </ul> <b>BV_DB_STAT</b> <ul style="list-style-type: none"> <li>• DELETE</li> <li>• INSERT</li> <li>• SELECT</li> <li>• SPROC</li> <li>• UPDATE</li> </ul> <b>BV_CACHE_STAT</b> <ul style="list-style-type: none"> <li>• BV_GDBQUERY_CACHE-HIT</li> <li>• BV_GDBQUERY_CACHE-MAX</li> <li>• BV_GDBQUERY_CACHE-MISS</li> <li>• BV_GDBQUERY_CACHE-SIZE</li> <li>• BV_GDBQUERY_CACHE-SWAP</li> <li>• BV_QUERY_CACHE-HIT</li> <li>• BV_QUERY_CACHE-MAX</li> <li>• BV_QUERY_CACHE-MISS</li> <li>• BV_QUERY_CACHE-SIZE</li> <li>• BV_QUERY_CACHE-SWAP</li> </ul>	<ul style="list-style-type: none"> <li>• CNT-AD-HIT</li> <li>• CNT-AD-MAX</li> <li>• CNT-AD-MISS</li> <li>• CNT-AD-SIZE</li> <li>• CNT-AD-SWAP</li> <li>• CNT-ALERTSCHED-HIT</li> <li>• CNT-ALERTSCHED-MAX</li> <li>• CNT-ALERTSCHED-MISS</li> <li>• CNT-ALERTSCHED-SIZE</li> <li>• CNT-ALERTSCHED-SWAP</li> <li>• CNT-CATEGORY_CONTENT-HIT</li> <li>• CNT-CATEGORY_CONTENT-MAX</li> <li>• CNT-CATEGORY_CONTENT-MISS</li> <li>• CNT-CATEGORY_CONTENT-SIZE</li> <li>• CNT-CATEGORY_CONTENT-SWAP</li> <li>• CNT-DF_GROUP-HIT</li> <li>• CNT-DF_GROUP-MAX</li> <li>• CNT-DF_GROUP-MISS</li> <li>• CNT-DF_GROUP-SIZE</li> <li>• CNT-DF_GROUP-SWAP</li> <li>• CNT-DF_MESSAGE-HIT</li> <li>• CNT-DF_MESSAGE-MAX</li> <li>• CNT-DF_MESSAGE-MISS</li> <li>• CNT-DF_MESSAGE-SIZE</li> <li>• CNT-DF_MESSAGE-SWAP</li> <li>• CNT-EDITORIAL-HIT</li> <li>• CNT-EDITORIAL-MAX</li> <li>• CNT-EDITORIAL-MISS</li> <li>• CNT-EDITORIAL-SIZE</li> <li>• CNT-EDITORIAL-SWAP</li> <li>• CNT-EXT_FIN_PRODUCT-HIT</li> <li>• CNT-EXT_FIN_PRODUCT-MAX</li> <li>• CNT-EXT_FIN_PRODUCT-MISS</li> <li>• CNT-EXT_FIN_PRODUCT-SIZE</li> <li>• CNT-EXT_FIN_PRODUCT-SWAP</li> <li>• CNT-INCENTIVE-HIT</li> <li>• CNT-INCENTIVE-MAX</li> <li>• CNT-INCENTIVE-MISS</li> <li>• CNT-INCENTIVE-SIZE</li> <li>• CNT-INCENTIVE-SWAP</li> </ul>	<ul style="list-style-type: none"> <li>• CNT-MSGSCHEM-HIT</li> <li>• CNT-MSGSCHEM-MAX</li> <li>• CNT-MSGSCHEM-MISS</li> <li>• CNT-MSGSCHEM-SIZE</li> <li>• CNT-MSGSCHEM-SWAP</li> <li>• CNT-MSGSCRIPT-HIT</li> <li>• CNT-MSGSCRIPT-MAX</li> <li>• CNT-MSGSCRIPT-MISS</li> <li>• CNT-MSGSCRIPT-SIZE</li> <li>• CNT-MSGSCRIPT-SWAP</li> <li>• CNT-PRODUCT-HIT</li> <li>• CNT-PRODUCT-MAX</li> <li>• CNT-PRODUCT-MISS</li> <li>• CNT-PRODUCT-SIZE</li> <li>• CNT-PRODUCT-SWAP</li> <li>• CNT-QUERY-HIT</li> <li>• CNT-QUERY-MAX</li> <li>• CNT-QUERY-MISS</li> <li>• CNT-QUERY-SIZE</li> <li>• CNT-QUERY-SWAP</li> <li>• CNT-SCRIPT-HIT</li> <li>• CNT-SCRIPT-MAX</li> <li>• CNT-SCRIPT-MISS</li> <li>• CNT-SCRIPT-SIZE</li> <li>• CNT-SCRIPT-SWAP</li> <li>• CNT-SECURITIES-HIT</li> <li>• CNT-SECURITIES-MAX</li> <li>• CNT-SECURITIES-MISS</li> <li>• CNT-SECURITIES-SIZE</li> <li>• CNT-SECURITIES-SWAP</li> <li>• CNT-TEMPLATE-HIT</li> <li>• CNT-TEMPLATE-MAX</li> <li>• CNT-TEMPLATE-MISS</li> </ul>
--	---	--

<ul style="list-style-type: none"> <li>• CNT-TEMPLATE-SIZE</li> <li>• CNT-TEMPLATE-SWAP</li> <li>• PARENTCATEGORY</li> <li>CACHE-HIT</li> <li>• PARENTCATEGORY</li> <li>CACHE-MAX</li> <li>• PARENTCATEGORY</li> <li>CACHE-MISS</li> <li>• PARENTCATEGORY</li> <li>CACHE-SIZE</li> <li>• PARENTCATEGORY</li> <li>CACHE-SWAP</li> </ul> <p><b>JS_SCRIPT_CTRL</b></p> <ul style="list-style-type: none"> <li>• CACHE</li> <li>• DUMP</li> <li>• FLUSH</li> <li>• METER</li> <li>• TRACE</li> </ul>	<p><b>BV_SMGR_STAT</b></p> <ul style="list-style-type: none"> <li>• CGI</li> <li>• CONN</li> <li>• IdIQ</li> <li>• JOB</li> <li>• MODE</li> <li>• Q_0</li> <li>• Q_1</li> <li>• Q_10</li> <li>• Q_11</li> <li>• Q_12</li> <li>• Q_13</li> <li>• Q_14</li> <li>• Q_15</li> <li>• Q_2</li> <li>• Q_3</li> <li>• Q_4</li> <li>• Q_5</li> <li>• Q_6</li> <li>• Q_7</li> <li>• Q_8</li> <li>• Q_9</li> <li>• SESS</li> <li>• THR</li> </ul>	<p><b>JS_SCRIPT_STAT</b></p> <ul style="list-style-type: none"> <li>• ALLOC</li> <li>• CTX</li> <li>• ERROR</li> <li>• FAIL</li> <li>• JSPERR</li> <li>• RELEASE</li> <li>• STOP</li> <li>• SUCC</li> <li>• SYNTAX</li> </ul> <p><b>BV_SMGR_QOS</b></p> <ul style="list-style-type: none"> <li>• ADMIN_CT</li> <li>• DEF_P</li> <li>• NEW_P</li> <li>• P_WEIGHT</li> <li>• REWARD_P1</li> <li>• REWARD_P2</li> <li>• REWARD_P3</li> <li>• REWARD_P4</li> <li>• REWARD_P5</li> </ul> <p><b>BV_SMGR_CTRL</b></p> <ul style="list-style-type: none"> <li>• DRAIN</li> </ul>
--	--	--

## Tips/Troubleshooting

### General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 9: Browsable Windows Performance Counter Monitor

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.

## To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click the required Microsoft Exchange Solution Template, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

## Tasks

### How to Configure the Browsable Windows Performance Counter monitor

#### 1. Prerequisites

- This monitor is only displayed in the user interface after deploying a Microsoft Exchange solution template (requires Trial, Premium, Ultimate, or System Collector edition).
- To enable the monitor, you must have an Operating System Instance (OSi) license with sufficient available capacity. For license purchase inquiries (or if you require additional capacity), contact your HPE sales representative or use the “Contact Us” link in the [HPE SiteScope Product page](#).

#### 2. Deploy the monitor using the Microsoft Exchange Solution Template

For details on using templates to deploy monitors, see *Deploying a SiteScope Solution Template in the Using SiteScope Guide*.

For details on the Microsoft Exchange solution template, see *Microsoft Exchange Solution Templates in the Using SiteScope Guide*.

#### 3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors.

Configure the monitor properties as required.

For a description of each setting, see the *UI Descriptions* section below.



## UI Descriptions

### Browsable Windows Performance Counter Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>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>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 <b>&lt;SiteScope root directory&gt;\templates.perfmon\browsable</b> directory under SiteScope. There are a number of default files in the standard SiteScope distribution.</p>
<b>Counters</b>	<p>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>Opens the Select Counters dialog box, enabling you to 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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 10: Check Point Monitor

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. The error and warning thresholds for the monitor can be set on one or more firewall statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Check Point monitor.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

## Tasks

### How to Configure the Check Point monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Check Point Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>Index</b>	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

UI Element	Description
<b>Community</b>	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>	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>	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>	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>	
<b>&lt;List of counters&gt;</b>	Displays the available server performance counters and those currently selected for this monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a> .

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- Dropped
- Logged
- Major
- Minor
- ModuleState
- PointEvent
- Product
- Rejected

# Chapter 11: Cisco Works Monitor

Use the Cisco Works monitor to monitor the content of event logs and other data from Cisco Works 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. The error and warning thresholds for the monitor can be set on one or more Cisco Works server statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Cisco Works monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" below](#)

### Supported Platforms/Versions

This monitor supports monitoring on Cisco Works 2000 servers and later.

### IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

## Tasks

### How to Configure the Cisco Works Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Tip:** The **SNMP Browser Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Browser Tool in the Using SiteScope Guide.

## UI Descriptions

### Cisco Works Monitor Settings

User interface elements are described below:

UI Element	Description
<b>SNMP Settings</b>	
<b>Server</b>	Name of the server you want to monitor.
<b>Port</b>	Port to use when requesting data from the SNMP agent. <b>Default value:</b> 161
<b>MIB file</b>	<p>MIB file display option.</p> <ul style="list-style-type: none"><li>• <b>CISCOWORKS-MIB</b> file causes only those objects that are described within that MIB file to be displayed.</li><li>• <b>All MIBs</b> causes all objects discovered on the given Cisco Works server to be displayed when browsing counters.</li></ul> <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>Performs 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>

UI Element	Description
<b>Starting OID</b>	<p>Use 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>You can 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> <p><b>Note:</b> This field is available in template mode only.</p>
<b>SNMP Connection Settings</b>	
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.</p> <p><b>Default value:</b> 5</p>
<b>Number of retries</b>	<p>Number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.</p> <p><b>Default value:</b> 1</p>
<b>Community</b>	<p>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.</p> <p><b>Default value:</b> public</p>
<b>SNMP version</b>	<p>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 setting fields below.</p> <p><b>Default value:</b> V1</p>
<b>Authentication algorithm</b>	<p>Authentication algorithm to use for version 3 connections.</p> <p><b>Default value:</b> MD5</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>User name</b>	<p>User name for version 3 connections.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>Password</b>	<p>Authentication password to use for version 3 connections.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>Privacy algorithm</b>	<p>The privacy algorithm used for authentication for SNMP version 3 (DES, 128-Bit AES, 192-Bit AES, 256-Bit AES).</p> <p><b>Default value:</b> DES</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>

UI Element	Description
<b>Privacy password</b>	Privacy password for version 3 connections. Leave blank if you do not want privacy. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Context name</b>	Context Name to use for this connection. This is applicable for SNMP V3 only. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Context engine ID</b>	Hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>SNMP Counters</b>	
<b>Counters</b>	Displays 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>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</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> </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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

SNMP data including the following categories and all of their metrics:

- applConformance
- applTable
- assocTable
- at
- egp
- egpNeighTable
- host
- icmp
- interfaces
- ip
- rdbmsConformance
- rdbmsObjects

- snmp
- system
- tcp
- udp

## Tips/Troubleshooting

### General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.



# Chapter 12: Citrix Monitor

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. The error and warning thresholds for the monitor can be set on one or more Citrix server performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Citrix monitor.

## Learn About

This section includes:

- ["What to Monitor" below](#)
- ["Supported Versions/Platforms" below](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)
- ["License Consumption" on the next page](#)

## What to Monitor

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 4.5 Administrator's Guide](http://support.citrix.com/article/CTX106319) (<http://support.citrix.com/article/CTX106319>), and about the Terminal Services Session Object at <http://msdn.microsoft.com/en-us/library/ms804500.aspx>.

## Supported Versions/Platforms

- 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, 4.x
  - Citrix XenApp 4.6, 5.0, 6.0, 6.5, 7.6

- This monitor is supported in SiteScopes running on Windows platforms, and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Enable SiteScope to Prefer IP Version 6 Addresses in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity Type License Usage
One point per metric	One OSi license per monitored host

# Tasks

## How to Configure the Citrix Monitor

### 1. Prerequisites

The following are important requirements for using the Citrix monitor:

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- SiteScopes running on Windows platforms need 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. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

- 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 478](#).

2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Citrix Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>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></p> <ul style="list-style-type: none"><li>• 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 Windows Monitoring in the Using SiteScope Guide.</li><li>• When working in template mode, 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></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

UI Element	Description
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 <a href="#">Configure SiteScope to Monitor Remote Windows Servers in the Using SiteScope Guide</a>.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see <a href="#">New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide</a>.</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>For information about the Citrix performance counters, see Appendix C of the <a href="#">MetaFrame Presentation Server 4.0 Administrator's Guide</a> (<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>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Objects" on the next page</a>.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see [Common Monitor Settings in the Using SiteScope Guide](#).

## Monitor Objects

Below is the list of Perfmon objects that can be configured for this monitor (if they are persist on the target machine):

Citrix IMA Networking	Citrix Subscription Store
Citrix MetaFrame Presentation Server	Citrix Subscription Store Synchronization
Citrix MetaFrame XP	Citrix XML Service
ICA Session	Citrix Xml Service Communication
Terminal Services Session	CitrixAdIdentityService
Terminal Services	CitrixAnalytics
Citrix Broker Service	CitrixConfigurationLogging
Citrix Credential Wallet	CitrixConfigurationService
Citrix Dazzle Resources Controller	CitrixDelegatedAdmin
Citrix Delegated Directory Claim Factory	CitrixEnvTest
Citrix Delegated Explicit Authentication	CitrixHostService
Citrix Delegated Kerberos Authentication	CitrixMachineCreationService
Citrix Delivery Services Web Application	CitrixMonitor
Citrix Explicit Core Citrix Receiver for Web	CitrixStorefront
Citrix Resource Subscription	Citrix CPU Utilization Mgmt User
Citrix Resources Common	Citrix Licensing
Citrix Saml11 Tokens	

## Tips/Troubleshooting

### General Tips/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 13: ColdFusion Server Monitor

Use the ColdFusion Server monitor to monitor the server performance statistics from ColdFusion 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. The error and warning thresholds for the monitor can be set on one or more ColdFusion server performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the ColdFusion Server monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption " on the next page](#)

## Supported Platforms/Versions

- This monitor supports monitoring ColdFusion 4.5.x, 9, 10, and 11 servers.
- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

## Tasks

### How to Configure the ColdFusion Server Monitor

#### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- SiteScopes running on Windows platforms need 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. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

#### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### ColdFusion Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>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>Note: When working in template mode, 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>

UI Element	Description
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 <a href="#">How to Configure SiteScope to Monitor a Remote Microsoft Windows Server</a> in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see <a href="#">New/Edit Microsoft Windows Remote Server Dialog Box</a> in the Using SiteScope Guide.</p>
<b>Version</b>	<p>Version of the ColdFusion Server you are monitoring (4.5x, 9, 10, 11).</p> <p><b>Default value:</b> 4.5x</p>
<b>Counters</b>	<p>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>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see [Common Monitor Settings](#) in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- Avg DB Time (msec)
- Avg Queue Time (msec)
- Avg Req Time (msec)
- Bytes In / Sec
- Bytes Out / Sec
- Cache Pops / Sec
- DB Hits / Sec
- Page Hits / Sec
- Queued Requests



- Running Requests
- Timed Out Requests

## Tips/Troubleshooting

### General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 14: COM+ Server Monitor

Use the COM+ Server monitor to monitor the performance of COM+ software components registered and running on Microsoft Windows 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the COM+ monitor.

## Learn About

### Supported Platforms/Versions

This monitor supports monitoring COM+ software components running on Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2 Update 1.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric Note: Additional licensing is required to enable this monitor type in the SiteScope interface after the free trial period expires.	One OSi license per monitored host. Note: Not available with Community edition.

## Tasks

### How to Configure the COM+ Monitor

#### 1. Prerequisites

There must be HTTP connectivity between the SiteScope server and the server running the COM+ probe.

#### 2. Install the COM+ probe

A COM+ probe component must be installed and running on the target COM+ server you want to monitor.

- Go to the [HPE Software Support site](#) (you need to enter your HPE user name and password).
- In the Search box, enter **COM+** and click **Search**.
- Download the COM+ probe from the results.
- After downloading, follow the instructions for installing the probe on the COM+ server to be monitored.

**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.

3. 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\**.

4. 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.

Configure the other COM+ Server monitor fields as described in the UI Descriptions section below.

## UI Descriptions

### COM+ Monitor Settings

User interface elements are described below:

UI Element	Description
<b>COM+ probe host name</b>	Host name of the COM+ probe.
<b>COM+ probe port number</b>	Port number of the COM+ probe. <b>Default value:</b> 8008
<b>Credentials</b>	Option for providing the user name and password authorization to the COM+ probe: <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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>HTTP proxy</b>	Domain name and port of an HTTP proxy server if a proxy server is used to access the probe.
<b>Proxy server user name</b>	Proxy user name if the proxy server requires a name and password to access the probe. Your proxy server must support Proxy-Authenticate for these options to function.

UI Element	Description
<b>Proxy server password</b>	Proxy password if the proxy server requires a name and password to access the probe.
<b>Timeout (seconds)</b>	<p>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 can 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>	Server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

Application Level	Transaction Level	Object Level (per object)
<ul style="list-style-type: none"><li>• Activation</li><li>• Authenticate</li><li>• Authenticate Failed</li><li>• Shutdown</li><li>• Thread Start</li><li>• Thread Terminate</li><li>• Work Enqueue</li><li>• Work Reject</li></ul>	<ul style="list-style-type: none"><li>• Transaction Aborted</li><li>• Transaction Commit</li><li>• Transaction Duration</li><li>• Transaction Prepared</li><li>• Transaction Start</li></ul>	<ul style="list-style-type: none"><li>• Disable Commit</li><li>• Enable Commit</li><li>• Object Activate</li><li>• Object Create</li><li>• Object Deactivate</li><li>• Object Destroy</li><li>• Object LifeTime</li><li>• Set Abort</li><li>• Set Complete</li></ul>

## Tips/Troubleshooting

### General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 15: Composite Monitor

This monitor enables you to monitor complex network environments by checking the status readings of a set of other SiteScope monitors, groups, or both. Each time the Composite monitor runs, it returns a status based on the number and percentage of items in the specified monitors, groups, or both, currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Composite monitor.

## Learn About

### What to Monitor

Use this monitor 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 permit, you can use the Composite monitor to create customized alert behavior.

### License Consumption

This monitor requires no additional licensing beyond the licensing requirements of the member monitors which it contains.

## Tasks

### How to Configure the Composite Monitor



Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## Composite Monitor Settings






User interface elements are described below:

UI Element	Description
<b>Items</b>	<p>Click the <b>Add</b>  button to open the Add Items dialog box, and select the groups, monitors, or both, that you want in the Composite monitor. For details on the Add Items dialog box, see <a href="#">"Add Items Dialog Box" below</a>. The Add Items dialog box displays all the monitors that are part of the same SiteScope.</p> <p>To remove items from the list, select the groups, monitors, or both, you want to remove (you can select multiple items using the CTRL or SHIFT keys), and click the <b>Delete</b>  button.</p> <p><b>Note when working in template mode:</b></p> <ul style="list-style-type: none"><li>• The monitors that you add to the Composite monitor are placeholders. They become real monitors when you deploy the Composite monitor.</li><li>• If you add the Composite monitor to a template, group, or subgroup, when you click the <b>Add Items</b> button, the Add Items dialog box displays only the monitors that are part of the same template as the new Composite monitor.</li></ul>
<b>Run monitors</b>	<p>The Composite monitor controls 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>Amount of time, in seconds, to wait between running each monitor (if <b>Run monitors</b> is selected).</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>All monitors in the 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

This dialog box enables you to select the monitors, groups, or both, that you want in the Composite monitor.

User interface elements are described below:

UI Element	Description
<b>Add Selected Items</b>	Click to add the selected groups, monitors, or both, to the Composite monitor.
 SiteScope	Represents the SiteScope root directory.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors).  If a group alert has been set up for the monitor group or subgroup, the alert  symbol is displayed next to the group icon.
	Represents a SiteScope monitor (enabled/disabled).  If an alert has been set up for the monitor, the alert  symbol is displayed next to the monitor icon.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Tips/Limitations

- 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.
- This monitor cannot be copied to a template. It must be created directly in a template.

# Chapter 16: CPU Monitor

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 need to create only 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the CPU monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["Status" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["Scheduling the Monitor" on the next page](#)
- ["License Consumption" on the next page](#)

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH (for details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide).
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

## 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 Windows, 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.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:



- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d

would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## 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 can 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.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor  Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

# Tasks

## How to Configure the CPU Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Tip:** The **Performance Counters Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Performance Counters Tool in the Using SiteScope Guide.

# UI Descriptions

## CPU Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>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></p> <ul style="list-style-type: none"><li>• Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li><li>• When configuring this monitor on SiteScopes running on UNIX versions, only remote servers that have been configured with an <b>SSH</b> connection method are displayed.</li><li>• When working in template mode, 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></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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>Notes:</b></p> <ul style="list-style-type: none"><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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</li></ul>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Tips/Troubleshooting

## General Tips/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- To get a detailed list of processes consuming most CPU resources, create an Email alert using the **WithDiagnostics** template. When the monitor reaches the configured threshold, CPU consumption for each process is sent in the body of the email alert.

## Monitor Specific Troubleshooting/Limitations

- If unable to monitor CPU usage on a Linux installation, check the **sysstat** package is deployed on the target Linux system.
- 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.

- When you run a CPU Monitor on a server that has no metrics, the calculated metric result that appears in the SiteScope Dashboard is n/a. If you then select a server that has metrics and run the monitor again, the calculated metric result remains n/a.

**Cause:** The CPU Monitor is not a dynamic monitor.

**Solution:** Create a new calculated metric for the monitor that has metrics and rerun the monitor.

- Incorrect CPU cores number is given when you run this monitor on an AIX operating system using multiple cores when CPU utilization is low, and simultaneous multithreading (SMT) is on.

**Cause:** If SMT is on (it is on by default in AIX), the CPU cores number will be multiplied by 2 or 4 depending on the hardware model and/or partition mode.

**Solution:** Turn SMT to off.

# Chapter 17: Custom Monitor

The Custom monitor broadens the capabilities of regular SiteScope monitors for tracking the availability and performance of monitored environments. The Custom monitor enables you to create your own monitor by developing a script that collects data from an application or a remote machine using custom Java or JavaScript code. The script then processes the data and creates metrics in names determined by you. You can use Java code developed by yourself or by a third-party to process the data.

You can share custom monitors by publishing them to the HPE Live Network community, enabling other SiteScope users to import the monitor template for their own use.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **Custom** monitor.

## Learn About

### Custom Monitor Overview

The Custom monitor enables you to develop your own monitor on top of the SiteScope infrastructure.

Custom monitors enable you to do the following:

- **Create monitors that provide additional metrics not available in existing monitors, and then process the collected data**

You can create your own monitor by developing a script that collects data using custom Java or JavaScript code, and then processes the data and creates metrics. Each time the Custom monitor runs, it updates the metrics and returns a status for the metrics defined in the script.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor API Reference (available from `<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip`).

- **Customize how results are displayed**

You can determine how results are displayed. For example, whether result data is displayed in megabytes or kilobytes.

- **Debug custom monitors offline**

You can perform offline debugging of a custom monitor script using a remote debugging server. This makes the script development process easier, since it enables you to complete the code and see the debugged data inside the script during the data processing stage. For details, see ["How to Debug a Custom Monitor Offline" on page 98](#).

After developing the monitor, you can:

- **Define thresholds for new metrics**

Because some metrics are defined only during a script run, you cannot define thresholds for them in advance. After the script has run for the first time and the metrics have been defined, you can then define thresholds for them. This provides more advanced data processing options than regular monitors. Note

that metrics can change between script runs, for example, where variables are used in metric names. Thresholds using a metric that does not exist after the monitor run are removed automatically.

- **Share the monitor with other SiteScope users**

After developing the monitor, you can export the monitor to a template, add external jars and/or classes if the monitor depends on them, and create a content package. The content package can then be sent to specific users, or shared with other SiteScope users by publishing it to the SiteScope community on [HPE Live Network](https://hpln.hpe.com/group/sitescope) (<https://hpln.hpe.com/group/sitescope>).

By sharing knowledge with other SiteScope users, you can benefit from extended SiteScope monitor coverage and the development of new monitors outside the SiteScope release cycle.

## License Consumption

Points-based Usage	Capacity-based Usage
One point for every 10 metrics. For example, 41 metrics consume 5 points.	One OSi per 15 monitors of this type.

## Tasks

This section includes:

- ["How to Develop a Custom Monitor" below](#)
- ["How to Debug a Custom Monitor Offline" on page 98](#)
- ["How to Access the Monitor Configuration Parameters Exposed in the Script" on page 99](#)
- ["How to Import and Use a Customizable Monitor" on page 100](#)

## How to Develop a Custom Monitor

### 1. Prerequisites

- You must be an advanced user SiteScope with knowledge of JavaScript.
- Knowledge of the application being monitored.

### 2. Create a Custom monitor

Create a group into which you want to add the custom monitor. Right-click the group, select **New > Monitor**, and select the **Custom** monitor. In the General Settings panel, enter a name and description for the monitor.

### 3. Create script parameters - optional

You can create a list of parameters that can be repeatedly used in the data processing script. To do so, enter the parameter name and value in the Script Parameters Table.

For example, you might want to create a host, user name, and password parameter. You can choose to hide parameter values, such as passwords, behind asterisks (\*\*\*\*\*) in the user interface. The hide option is editable when working in template mode only.

For user interface details, see the UI Descriptions section below.

**Note:** By default, the maximum number of parameters allowed in the table is 10. When the

maximum number of rows is reached, no additional rows can be added. You can modify this number by changing the **Custom monitor maximum number of script parameters** value in **Preferences > Infrastructure Preferences > Custom Settings**. You must restart SiteScope if you change this setting.

#### 4. Create the data processing script

In the **Data Processing Script** area of Custom Monitor Settings, create the script that parses the results and creates new metrics according to the name that you determined.

For details on the monitor configuration properties, including how to access them, and the monitor storage and metrics names, see "[How to Access the Monitor Configuration Parameters Exposed in the Script](#)" on page 99.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor API Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**). A sample jar file showing the custom monitor's capability to access Java code is provided in the **<SiteScope root directory>\examples\monitors\custom\lib** folder.

For details on scripting in Java, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

##### Tip:

- A sample Custom monitor script is provided in the **Data Processing Script** box. To use it, you need to uncomment the script.
- Sample scripts for all the custom monitors are available from the sample content package located in the **<SiteScope installation directory>\examples\monitors\custom** folder. **CustomMonitorSamplePackage.zip** contains examples for SiteScope 11.20, and **CustomMonitorsExamples\_11\_21.zip** contains updated examples including a Custom Database monitor with a dynamic query, a manifest file created using the Export Content Package Wizard, and template mail and template mail subject files. To use these scripts, you need to import the custom monitor content package and then deploy the custom monitor template. For task details, see steps 3 and 4 of "[How to Import and Use a Customizable Monitor](#)" on page 100.

##### Note:

- If your monitor needs to open a network connection to another server from the data processing script or the Java code that is called from the script, you must enable the **Allow network access** setting in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- Access for the data processing script is restricted to the following folders/files on the SiteScope server:
  - The **\conf** folder which is located inside each content package (**<SiteScope root directory>\packages\imported** or **<SiteScope root directory>\packages\workspace**) (requires *Read* permissions).
  - **<SiteScope root directory>\logs\custom\_monitors\\*** (all permissions)
- You can use the **custom\_monitor.log** file for any info, warning, error, and debug messages that you want to write during the execution of the script. The log is located in **<SiteScope root**

**directory>\logs\custom\_monitors**. For details on changing the log to DEBUG mode, see ["Custom Monitor Logs" on page 104](#).

- By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the **Maximum number of counters** value in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- When working in template mode, you can use template variables in a data processing script.

## 5. Generate a path for storing the files used for creating the Custom monitor

Click the **Create Path** button to create a folder where the relevant jars, classes, configuration, and template files required for running the monitor can be saved. A folder with a relative path is created under **<SiteScope root directory>\packages\workspace\package\_<Package ID>**. The path is displayed as read only.

The folder contains the following (empty) subfolders:

- **packages\workspace\package\_<>\lib**. Used for storing external jar files used by the monitor script.
- **packages\workspace\package\_<>\classes**. Used for storing compiled Java classes; note that they should be copied with the entire package folder structure.
- **packages\workspace\package\_<>\conf**. Used for storing configuration files, documentation, and XML files.
- **packages\workspace\package\_<>\template**. Used for storing the template files that contain the custom monitor (you perform this in ["Create a monitor template - optional" on the next page](#)).

You can copy the required files to these folders at this stage, or when performing ["Create a content package - optional" on the next page](#).

**Note:** If you add or modify jars/classes after the first monitor run, you must either:

- Restart SiteScope for the changes to take effect, or
- To avoid having to restart SiteScope, you should enable the **Reload classes and jars on each monitor run** option in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. This option should only be used during script development, and should be cleared in the production stages since it impacts performance.

## 6. Configure topology reporting - optional

To report monitor and related CI topology data to BSM's RTSM, configure the required topology reporting settings as described in [How to Configure Topology Reporting for a Custom Monitor in the Using SiteScope Guide](#).

## 7. Configure other settings for the monitor - optional

Configure other settings for the monitor as required. For details, see [Common Monitor Settings in the Using SiteScope Guide](#).

## 8. Save the monitor and wait for the first monitor run

Save the monitor. SiteScope verifies the correctness of the monitor configuration both locally and on the

remote server to be monitored, before saving the settings, regardless of whether you clicked **Verify & Save** or **Save**.

The monitor collects data and filters it based on the script you supplied.

## 9. Managing custom monitors

After creating a custom monitor, you can copy, move, or delete the monitor. When doing so, this affects the content package folder (created in the **<SiteScope root directory>\packages\workspace** directory) as follows:

Action	File System Impact
Copy Monitor	Makes a copy of the content package folder in the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder.
Cut Monitor	No change.
Delete Monitor	If you delete the custom monitor, the content package folder is removed from the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder of the SiteScope file system.
Deploy template with custom monitor + content package	No change. If a deployed monitor is copied, the content package will be copied to the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder of the SiteScope file system.

## 10. Define thresholds for the metrics - optional

After the monitor has run, you can:

- Make changes to the script and define thresholds for metrics that were created or updated in the run. For details, see Threshold Settings in the Using SiteScope Guide.
- Check status and values of the metrics in the SiteScope Dashboard.
- Set up alerts on the monitor. For details, see How to Configure an Alert in the Using SiteScope Guide.

## 11. Create a monitor template - optional

- a. To copy the monitor to a template, right-click the monitor, select **Copy to Template**, and select the template group to which you want to add the copied configuration. For details, see How to Create a Template by Copying Existing Configurations in the Using SiteScope Guide.
- b. Make any necessary changes such as adding template variables to the template. For details on template variables, see New Variable Dialog Box in the Using SiteScope Guide.

## 12. Create a content package - optional

- a. Copy the files used for creating the monitor to the predefined content package subfolders:
  - **<SiteScope>\packages\workspace\package\_<Package ID>\lib**. (Optional) Copy any external jars used by the custom monitor script to this folder. Java classes from the jar files can be accessed from the data processing script. Note that you can use this monitor without external jars.

**Note:** In the data processing script, to import a package from a jar that does not start with



```
com., org., or java., you must add the package's prefix:  
importPackage(Packages.<packageName>)
```

For example, `importPackage(Packages.it.companyname.test);`

For details on importing Java classes and packages, see  
<http://www.mozilla.org/rhino/ScriptingJava.html>.

- **<SiteScope>\packages\workspace\package\_<>\classes**. (Optional) Copy the compiled Java classes with the entire package folder structure to this folder; this is not required if the class files were packaged in a jar that was copied to the `\lib` folder. The class files can be accessed from the data processing script.
- **<SiteScope>\packages\workspace\package\_<>\conf**. (Optional) Copy the configuration files, documentation, and XML files to this folder.
- **<SiteScope>\packages\workspace\package\_<>\template**. (Optional) The folder should contain the template files exported from SiteScope (performed in "[Create a monitor template - optional](#)" on the previous page). Each template can contain various types of monitors, custom and regular.

b. Copy extension files - optional

If the monitor references script or alert extension files in the SiteScope file system, copy them to the relevant folders in **<SiteScope root directory>\packages\workspace\extensions**:

- **\scripts**. Used for storing script files that are used to run shell commands or other scripts on the machine where SiteScope is running.
- **\scripts.remote**. Used for storing script files that are used for running a script that is stored on a remote machine.
- **\templates.mail**. Used for storing the file containing the format and content of alert messages sent by email.
- **\templates.mail.subject**. Used for storing the file containing the subject line of alert messages sent by email.
- **\templates.mib**. Used for storing the MIB files that are used to create a browsable tree that contains names and descriptions of the objects found during a traversal.
- **\templates.os**. Used for storing the shell commands to be run when monitoring remote UNIX servers.

**Note:**

- On exporting the files to a content package, the unique package ID is added to the script and template files as a suffix (before the file extension) under the relevant folder in the SiteScope root directory.
- As part of the import process, the **template.os** and **templates.mib** files are edited and the unique package ID is added to some properties inside the files.

c. Export the content package to a zip file

Select the **Templates** context. In the template tree, right-click the template or template container that you want to export to a content package, and select **Export > Content Package**.

In the Export Content Package Wizard, enter details of the content package (manifest), and select the templates and files associated with these templates to include. For Wizard details, see Export Content Package Wizard.

For task details, see How to Create, Export, and Import a Custom Monitor Content Package and How to Create, Export, and Import a Template Extension Content Package in the Using SiteScope Guide.

**Note:** The Select Files page of the Wizard displays files from the **<SiteScope root directory>\packages\workspace\package\_<Package ID>** and **<SiteScope root directory>\packages\workspace\extensions** folders listed above, except for the **\META-INF** and **\templates** folders which are not displayed.

### 13. Share the custom monitor with other SiteScope users - optional

You can distribute a content package zip file by:

- Sending it to individual SiteScope users.
- Sharing it with other SiteScope users by uploading it to the Community Content for SiteScope page on [HPE Live Network](https://hpln.hpe.com/group/sitescope) (<https://hpln.hpe.com/group/sitescope>). HPE Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HPE Software portfolio.

For task details, see How to Publish Content to the HPE Live Network Community.

## How to Debug a Custom Monitor Offline

This task describes the steps involved in offline debugging of a custom monitor script using a remote debugging environment. This makes the script development process easier, since it enables you to complete the code and see the debugged data inside the script during the data processing stage.

#### 1. Prerequisites

To perform offline debugging, the Eclipse IDE with Web Tools must be installed on a local machine.

#### 2. In SiteScope, enable the global custom monitor debugging setting in SiteScope Preferences

Select **Preferences > Infrastructure Preferences > Custom Monitor Settings**, and select the **Enable custom monitor debugging** check box.

#### 3. In SiteScope, create a custom monitor with offline debugging enabled

Create a custom monitor. For details, see the previous task.

When configuring the monitor settings, expand **Custom Monitor Settings**, and under the Data Processing Script section, select **Enable monitor debugging**.

Save the monitor.

#### 4. Copy the Custom Monitor Debugging Eclipse project to the debugging environment

The Custom Monitor Debugging Eclipse project is available (in zip format) from:

- **<SiteScope root directory>\examples\monitors\custom\CustomMonitorDebuggingEclipseProject**.
- The Community Content for SiteScope page on the HPE Live Network (<https://hpln.hp.com/group/community-content-sitescope>).

**Note:** Make sure you use the correct version of the Custom Monitor Debugging Eclipse project. SiteScope 11.23 is compatible with version 2.0 of the project (**SISProxy-2.0.min.js**).

#### 5. Import the Custom Monitor Debugging project into Eclipse IDE

- a. On the debugging environment, open Eclipse IDE and click **Import**.
  - b. Select **General > Existing Project into Workspace**, and click **Next**.
  - c. Select the Custom Monitor Debugging Eclipse project (zip file).
6. Copy the SiteScope Custom Monitor Data Processing Script to the Custom Monitor Debugging project
  - a. Copy the content of Data Processing Script from the SiteScope custom monitor to **MonitorScript.js** script.
  - b. Connect to the SiteScope monitor by entering the following in the **DebugConfiguration.js** file:
    - **host**. Name of the SiteScope server.
    - **port**. Port used by the SiteScope server.
    - **username**. Username for accessing the SiteScope server.
    - **password**. Password to access the SiteScope server.
    - **monitorPath**. Full path to the custom monitor to debug in SiteScope including the monitor name, separated by "/". For example, Group1/Group2/Group3/Custom Monitor Name.
7. Enable the debugger to use external jar files - optional (where the script uses external jar files)

If the monitor script uses external jar files, copy the jar files from **<SiteScope root directory>\packages\workspace\package\_<Package ID>\lib** to the **<JRE installation path>\lib\ext** directory on the debugging environment.
8. Run the debugger
  - a. In the Eclipse IDE, select **Debug Configuration**.
  - b. Select **Rhino JavaScript > Custom Monitor Debugging - MonitorScript.js**.
  - c. The debugger connects to SiteScope, and runs the script within the monitor.

SiteScope returns the data to the debugger and then disconnects. This enables the debugger to simulate the script running the same data.
9. Debug the script

Use Eclipse IDE to debug the script.

## How to Access the Monitor Configuration Parameters Exposed in the Script

### Data Processing Script:

- You can access the configuration parameters for custom monitors in the data processing script using:

```
myContext.getInputData().getConfigurationParameter("<configuration parameter name>");
```

Example:

```
var monitorName = myContext.getInputData().getConfigurationParameter("monitorName");
```

The following monitor properties are exposed to the script (for all custom monitors):

- `monitorName`. The name of the monitor.
- `monitorDescription`. A description of the monitor.
- No additional properties are exposed for the Custom Monitor.
- You can set the summary string which is used as the monitor status in the SiteScope Dashboard using:

```
myContext.getScriptResult().setSummary("<text summary>");
```

The default value is: `summary = <a set of metrics and their values>`
- You can set monitor availability which is displayed in the SiteScope Dashboard using:

```
myContext.getScriptResult().setAvailability(<true/false>)
```

The default value is: `availability = true`

### Topology Script:

You can access the configuration parameters for custom monitors in the topology script using:

```
Framework.getDestinationAttributeAsObject("configuration").get("<configuration parameter name>")
```

To access data saved in the monitor storage (this is a place where you can save script data for use in future executions):

```
Framework.getDestinationAttributeAsObject("monitorStorage").get("<configuration parameter name>")
```

To access the list of metric names used in the script:

```
Framework.getDestinationAttributeAsObject("metrics")
```

## How to Import and Use a Customizable Monitor

After developing a custom monitor and creating a content package zip file, the content package can then be sent to specific users, or be published to the [HPE Live Network](https://hpln.hpe.com/group/sitescope) (<https://hpln.hpe.com/group/sitescope>) community enabling other users to import the monitor for their own use.

For details on using the Wizard, see Export Content Package Wizard.

### 1. Prerequisites

Only a SiteScope administrator user, or a user granted the **Add, edit or delete templates** permissions can import monitor templates from a content package. For details, see Permissions.

### 2. Access the custom monitor content package

- If a content package zip file was sent to you, skip to the next step.
- If a content package was made available to the Community Content for SiteScope page on [HPE Live Network](https://hpln.hpe.com/group/sitescope), download the content package to your SiteScope machine. HPE Live Network is an online community providing a central location for HPE customers to share information and learn about add-on content, extensions and related activities across the HPE Software portfolio.

For task details, see How to download a template or content package from the HPE Live Network in the Using SiteScope Guide.

### 3. Import the custom monitor content package

- a. In SiteScope, select the **Templates** context. In the template tree, right-click the template container into which you want to import the content package, and click **Import**.
- b. In the Content Import dialog box, select **Content package**, and click the **Browse** button. Navigate to the folder containing the package you want to import (packages are distributed in zip format). Click **Open**, and then click **OK**. For details on the Content Import dialog box, see Content Import Dialog Box in the Using SiteScope Guide.

For task details, see How to Create, Export, and Import a Custom Monitor Content Package and How to Create, Export, and Import a Template Extension Content Package in the Using SiteScope Guide.

### 4. Verify the template was imported successfully by checking it was added to the template tree

The content package is copied to the **<SiteScope root directory>\packages\imported** folder, and a new folder is created with the name: **<Package/Zip Name>.zip\_<Package ID>**.

The folder contains:

- **\META-INF**. Contains the manifest file where information about the content package is stored.
- **\templates**. Contains files from which templates in this content package were imported into SiteScope.
- **<Package/Zip Name>**. Uncompressed package that contains the above-mentioned folders, the **\extensions** folder which contains script and alert template files referenced by monitors in the imported templates, and the folders used for Custom monitors:
  - **\classes**. Used for storing compiled Java classes.
  - **\conf** Used for storing configuration files, documentation, and XML files.
  - **\lib** Used for storing external jar files used by the monitor script. Note that the **\lib** folder is shared between all monitors imported in the same template.
- **<Package/Zip Name>.zip.properties**. This is the descriptor (manifest) file for content packages created in SiteScope 11.20, that is used in case of rollback, uninstall, or upgrade. The file contains the ID of the SiteScope template that was deployed, the location of the files in SiteScope, and other information about the content package.

The imported templates and dependency files can be used directly or modified as required.

Where script or alert templates are referenced in the user interface, the unique package ID is added as a suffix.

**Example:** ShortMail alert action template referenced in the Template field.

The screenshot shows a web-based form titled "Action Type Settings". It contains several input fields with labels: "Action name:" (value: "EMail"), "\* Recipients:" (value: "Default"), "Addresses:" (empty), "\* Subject:" (value: "Typical"), and "\* Template:" (value: "ShortMail\_06b62f60-807c-4102-adea-9a7ebdd80e8b"). The "Template" field is highlighted with a red rectangular box.

## 5. Deploy the custom monitor template

After importing the custom monitor template, you can deploy the template to a group.

- In the template tree, right-click the custom monitor 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 user interface details, see Select Group Dialog Box in the Using SiteScope Guide.
- In the Deployment Values dialog box, enter the required variable values in the entry boxes displayed, and click **OK**. The entry boxes displayed correspond to the template variables used in the template objects. For user interface details, see Deployment Values Dialog Box in the Using SiteScope Guide.

**Note:** When deploying the template or publishing changes in the template to deployed groups, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, because the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.

- d. Verify that the template was deployed successfully (the template objects should be added to the specified group in the monitor tree).

For task details, see *How to Deploy Templates Using the User Interface* in the *Using SiteScope Guide*.



## 6. Configure monitor status thresholds

After the monitor run, you can define thresholds for metrics that were resolved in the run. In the **Threshold Settings** panel of the custom monitor, select metrics for which you want to define thresholds in the **Condition** column by using variables or free text, or selecting default metrics from the drop-down list, and enter the value applicable to the metric parameter.

# UI Descriptions

## Custom Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Script Parameters Table</b>	
	<b>Add Parameter.</b> Adds a new line to the Script Parameters table, enabling you to define parameters for use in the custom monitor script.
	<b>Delete Parameter.</b> Deletes the selected parameter.
<b>Parameter Name</b>	The name assigned to the parameter. All parameter names must be different.
<b>Parameter Value</b>	The parameter value.  If you want to hide a parameter value such as a password, select the <b>Hide Value</b> check box. The value is masked behind asterisks (*****) in the user interface.
<b>Hide Value</b>	Select to hide the parameter value in the Script Parameters table and in the custom monitor script. The value is masked behind asterisks (*****).  This option is useful for an administrator in SiteScope when creating custom monitor templates, since it enables the monitor to be deployed without the parameter value being displayed in the monitor view.  <b>Default value:</b> Not selected  <b>Note:</b> The hide option is editable when working in template mode only.

UI Element	Description
<b>Configuration File</b>	Use the <b>Browse</b> button to select the configuration file. The configuration file must be a valid XML file. If it is not, then an error message is displayed. The XML configuration file is copied into the <code>conf</code> folder of the monitor.
<b>Data Processing Script</b>	
<b>&lt;Script&gt;</b>	<p>The input data for the data processing script is displayed in this box.</p> <p>Define the script that parses the results and creates new metrics. For details on the monitor configuration properties in the script, including how to access them, and the monitor storage and metrics names, see <a href="#">"How to Access the Monitor Configuration Parameters Exposed in the Script" on page 99</a>.</p> <p><b>Note:</b> By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the <b>Maximum number of counters</b> value in <b>Preferences &gt; Infrastructure Preferences &gt; Custom Monitor Settings</b>.</p>
<b>Package path</b>	<p>Path generated by SiteScope where the files used for developing the monitor can be saved. This enables you to add the jars on which the monitor depends (if applicable), classes, configuration, and templates files to the monitor. The path is displayed as read only.</p> <p>Click the <b>Create Path</b> button to create a folder with a relative path in the SiteScope root directory (<code>packages\workspace\package_&lt;unique ID&gt;</code>). The path is displayed as read only.</p> <p>The folder contains the following subfolders into which you copy the files used to create the monitor:</p> <ul style="list-style-type: none"> <li>• <b>lib.</b> (Optional) Used for storing external jar files used by the monitor script. Note that you can use this monitor without external jars.</li> <li>• <b>classes.</b> (Optional) Used for storing Java compiled classes; note that they should be copied with the entire package folder structure.</li> <li>• <b>conf.</b> (Optional) Used for storing configuration files, documentation, and XML files.</li> <li>• <b>template.</b> (Mandatory) Used for storing the template files that contain the custom monitor. It must contain at least one template. Each template can contain various types of monitors; custom and regular.</li> </ul> <p><b>Note:</b> This field is displayed when working in monitor mode only. When working in template mode and the monitor is deployed, the content pack is imported into the path.</p> <p><b>Enable monitor debugging:</b> Select the checkbox to enable sending debugging logs for custom monitors to a remote debugging server. Note that custom monitor debugging must also be enabled in <b>Infrastructure Preferences. (Infrastructure Preferences &gt; Custom Monitor Settings &gt; Enable custom monitor debugging)</b>.</p>
<b>Checksum</b>	Click <b>Calculate Checksum</b> to calculate the MD5 checksum of a specific folder and the script.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and limitations for the Custom monitor.

- ["General Tips/Limitations" below](#)
- ["Custom Monitor Logs" below](#)

### General Tips/Limitations

- If a user-defined or imported Java package has the same name as an existing SiteScope or standard Java package, SiteScope ignores the user-defined/imported Java package.
- When setting custom monitor metrics with a string (non-numeric) value, the maximum and average values in the Measurement Summary table of the Management Report are shown as 'n/a'. This also occurs if you change the metric value type, for example, if you set the metric with a numeric value, and later change it to a string value or vice versa.
- When deploying a custom monitor using a template, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, because the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.
- When publishing changes to a template that contains a custom monitor, we recommend using the **Disable custom monitors while publishing changes** option (selected by default) in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. The monitor is temporarily disabled before changes are published and is restored to the enabled state after changes have been made.
- Setting status thresholds using a baseline is not supported on user-defined metrics.
- You can use third-party .jar files without removing the JVM security from the registry by adding the `_scriptSandboxRuntimePermissions` property to the `<SiteScope root directory>\groups\master.config` file, and specifying the permitted jar files. For example, to use signed libraries `jopcagtbases.jar` and `jopcagtmsgs.jar`, configure the parameter as follows: `_scriptSandboxRuntimePermissions=loadLibrary.jopcagtbases, loadLibrary.jopcagtmsgs`.  
For the types of runtime permissions that can be used, see Runtime Permission class in the [Java API documentation](http://docs.oracle.com/javase/7/docs/api/java/lang/RuntimePermission.html) (<http://docs.oracle.com/javase/7/docs/api/java/lang/RuntimePermission.html>).

### Custom Monitor Logs

- Errors in the monitor (including errors in the script) are written to the SiteScope logs in the same way as for any other monitor. Check the **error.log** and **RunMonitor.log** files.
- Error messages from the script are displayed in the **custom\_monitor.log** file located in `<SiteScope root directory>\logs\custom_monitors`. This log can be used for info, warning, error, and debug messages from running the script.

To change the log level to **DEBUG** mode, in `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties`, change `$(loglevel)` to **DEBUG** in the following paragraph:

```
# Custom monitors category
log4j.category.CustomMonitor=$(loglevel),custom.monitor.appender
log4j.additivity.CustomMonitor=false change
```



# Chapter 18: Custom Database Monitor

The Custom Database monitor broadens the capabilities of database monitors which are used to monitor the availability and performance of your systems and applications, whose data is accessible through database queries. Using the Custom Database monitor, you can create your own database monitor by developing queries that collect data, and a script that processes the collected data and creates metrics. You can use Java code developed by yourself or by a third-party to process the data.

You can share custom monitors by publishing them to the HPE Live Network community, enabling other SiteScope users to import the monitor template for their own use.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **Custom Database** monitor.

## Learn About

This section includes:

- ["Custom Database Monitor Overview" below](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)
- ["License Consumption" on the next page](#)

## Custom Database Monitor Overview

The Custom Database monitor enables you to develop your own database monitor on top of the SiteScope infrastructure. This provides you with greater flexibility not available in existing monitors.

You can use the Custom Database monitor to:

- **Collect any database data you like**

You can create a series of SQL queries for the database tables you want to monitor. SiteScope runs the queries and returns the results to the monitor in an object that contains a set of results for each query. Each time the monitor runs, it re-runs your queries and collects fresh data.

- **Process the collected data**

You can create a script in the monitor that can extract and process the results of the collected data. For example, you can define metrics based on collected data from the database and perform mathematical operations on it as in the sample script provided.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor API Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**).

- **Collect data dynamically**

You can include dynamically-defined queries in the data processing script. These queries are executed while the script is running, in contrast to predefined queries, which are executed before the script is run. Dynamically-executed queries provide the added benefit of enabling you to create queries based on values that are not in the monitored entity data store (for example, timestamp), create queries based on previous

query results or calculations, and include variables in queries. For details, see [Data Processing Script with Dynamic Queries](#) in the [Using SiteScope Guide](#).

- **Debug custom monitors offline**

You can perform offline debugging of a custom monitor script using a remote debugging server. This makes the script development process easier, since it enables you to complete the code and see the debugged data inside the script during the data processing stage. For details, see ["How to Debug a Custom Monitor Offline"](#) on page 112.

After developing the monitor, you can:

- **Define thresholds for new metrics**

Because some metrics are defined only during a script run, you cannot define thresholds for them in advance. After the script has run for the first time and the metrics have been defined, you can then define thresholds for them. This provides more advanced data processing options than regular monitors. Note that metrics can change between script runs, for example, where variables are used in metric names. Thresholds using a metric that does not exist after the monitor run are removed automatically.

- **Share the monitor with other SiteScope users**

After developing the monitor, you can export the monitor to a template, add external jars and/or classes if the monitor depends on them, and create a content package. The content package can then be sent to specific users, or shared with other SiteScope users by publishing it to the SiteScope community on [HPE Live Network](#) (<https://hpln.hpe.com/group/sitescope>).

By sharing knowledge with other SiteScope users, you can benefit from extended SiteScope monitor coverage and the development of new monitors outside the SiteScope release cycle.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports IPv6 addresses in the TCP (JDBC) protocol. Support for IPv6 might also depend on the JDBC driver being used.

For details on using IPv6, see [Support for IP Version 6](#) in the [Using SiteScope Guide](#).

## License Consumption

Points-based Usage	Capacity-based Usage
One point for every 10 metrics. For example, 41 metrics consume 5 points.	One OSi license per monitored host.

## Tasks

This section includes:

- ["How to Develop a Custom Database Monitor"](#) on the next page
- ["How to Debug a Custom Monitor Offline"](#) on page 112
- ["How to Access the Monitor Configuration Parameters Exposed in the Script"](#) on page 113
- ["How to Import and Use a Custom Database Monitor"](#) on page 114

## How to Develop a Custom Database Monitor

### 1. Prerequisites

- You must be an advanced SiteScope user with knowledge of JavaScript.
- Knowledge of SQL and the database systems being monitored.
- The database monitoring environment must be configured as described in ["How to Configure the Database Query Monitoring Environment" on page 172](#) (ignore the last step in the referenced task).

### 2. Create a Custom Database monitor with the relevant database queries

- a. Create a group into which you want to add the custom monitor. Right-click the group, select **New > Monitor**, and select the **Custom Database** monitor.
- b. Configure the monitor properties:
  - In the **General Settings** panel, enter a name and description for the monitor.
  - In the **Main Settings** area of Custom Database Monitor Settings, configure the monitor properties as described in the UI Descriptions section below.
  - In the **Queries** table, enter a separate query for each database instance and table in the database you want to monitor.

**Tip:** By default, you can enter up to 10 queries in the table. You can modify the number of queries that can be added to the table in **Preferences > Infrastructure Preferences > Custom Monitor Settings** by configuring the **Maximum number of queries** value.

### 3. Create script parameters - optional

You can create a list of parameters that can be repeatedly used in the data processing script. To do so, enter the parameter name and value in the Script Parameters Table.

For example, you might want to create a host, user name, and password parameter. You can choose to hide parameter values, such as passwords, behind asterisks (\*\*\*\*\*) in the user interface. The hide option is editable when working in template mode only.

For user interface details, see the UI Descriptions section below.

**Note:** By default, the maximum number of parameters allowed in the table is 10. When the maximum number of rows is reached, no additional rows can be added. You can modify this number by changing the **Custom monitor maximum number of script parameters** value in **Preferences > Infrastructure Preferences > Custom Settings**. You must restart SiteScope if you change this setting.

### 4. Create the data processing script

In the **Data Processing Script** area of Custom Database Monitor Settings, create the script that parses the results and creates new metrics in the names that you determined.

In addition, you can include any number of queries in the script. The queries are executed as the script is run, which means that the monitor collects fresh data from the database being monitored. After the data is retrieved, it becomes available for the script to use. A query in a script has the same syntax as a query defined in the queries table, but it can be structured using variables which makes it dynamic within the monitor run context. For details on dynamic queries, see *Data Processing Script with Dynamic Queries* in the *Using SiteScope Guide*.

For details on the monitor configuration properties, including how to access them, and the monitor storage and metrics names, see ["How to Access the Monitor Configuration Parameters Exposed in the Script" on page 113](#).

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor API Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**). A sample jar file showing the custom monitor's capability to access Java code is provided in the **<SiteScope root directory>\examples\monitors\custom\lib** folder.

For details on scripting in Java, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

**Tip:**

- A sample Custom Database monitor script is provided in the **Data Processing Script** box. To use it, you need to uncomment the script.
- Sample scripts for all the custom monitors are available from the sample content package located in the **<SiteScope installation directory>\examples\monitors\custom** folder. **CustomMonitorSamplePackage.zip** contains examples for SiteScope 11.20, and **CustomMonitorsExamples\_11\_21.zip** contains updated examples including a Custom Database monitor with a dynamic query, a manifest file created using the Export Content Package Wizard, and template mail and template mail subject files. To use these scripts, you need to import the custom monitor content package and then deploy the custom monitor template. For task details, see steps 3 and 4 of ["How to Import and Use a Custom Database Monitor" on page 114](#).

**Note:**

- If your monitor needs to open a network connection to another server from the data processing script or the Java code that is called from the script, you must enable the **Allow network access** setting in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- Access for the data processing script is restricted to the following folders/files on the SiteScope server:
  - The **\conf** folder which is located inside each content package (**<SiteScope root directory>\packages\imported** or **<SiteScope root directory>\packages\workspace**) (requires *Read* permissions).
  - **<SiteScope root directory>\logs\custom\_monitors\\*** (all permissions)
- You can use the **custom\_monitor.log** file for any info, warning, error, and debug messages that you want to write during the execution of the script. The log is located in **<SiteScope root directory>\logs\custom\_monitors**. For details on changing the log to DEBUG mode, see ["Custom Monitor Logs" on page 121](#).
- By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the **Maximum number of counters** value in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- When working in template mode, you can use template variables in a data processing script.

## 5. Generate a path for storing the files used for creating the Custom Database

## monitor

Click the **Create Path** button to create a folder where the relevant jars, classes, configuration, and template files required for running the monitor can be saved. A folder with a relative path is created under **<SiteScope root directory>\packages\workspace\package\_<Package ID>**. The path is displayed as read only.

The folder contains the following (empty) subfolders:

- **packages\workspace\package\_<>\lib**. Used for storing external jar files used by the monitor script.
- **packages\workspace\package\_<>\classes**. Used for storing compiled Java classes; note that they should be copied with the entire package folder structure.
- **packages\workspace\package\_<>\conf**. Used for storing configuration files, documentation, and XML files.
- **packages\workspace\package\_<>\template**. Used for storing the template files that contain the custom monitor (you perform this in ["Create a monitor template - optional" on the next page](#)).

You can copy the required files to these folders at this stage, or when performing ["Create a content package - optional" on the next page](#).

**Note:** If you add or modify jars/classes after the first monitor run, you must either:

- Restart SiteScope for the changes to take effect, or
- To avoid having to restart SiteScope, you should enable the **Reload classes and jars on each monitor run** option in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. This option should only be used during script development, and should be cleared in the production stages since it impacts performance.

### 6. Configure topology reporting - optional

To report monitor and related CI topology data to BSM's RTSM, configure the required topology reporting settings as described in [How to Configure Topology Reporting for a Custom Monitor in the Using SiteScope Guide](#).

### 7. Configure other settings for the monitor - optional

Configure other settings for the monitor as required. For details, see [Common Monitor Settings in the Using SiteScope Guide](#).

### 8. Save the monitor and wait for the first monitor run

Save the monitor. SiteScope verifies the correctness of the monitor configuration both locally and on the remote server to be monitored, before saving the settings, regardless of whether you clicked **Verify & Save** or **Save**.

The monitor collects data from the database instances, and filters the data based on the script you supplied.

### 9. Managing custom monitors

After creating a custom monitor, you can copy, move, or delete the monitor. When doing so, this affects the content package folder (created in the **<SiteScope root directory>\packages\workspace** directory) as follows:

Action	File System Impact
Copy Monitor	Makes a copy of the content package folder in the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder.
Cut Monitor	No change.
Delete Monitor	If you delete the custom monitor, the content package folder is removed from the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder of the SiteScope file system.
Deploy template with custom monitor + content package	No change. If a deployed monitor is copied, the content package will be copied to the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder of the SiteScope file system.

## 10. Define thresholds for the metrics - optional

After the monitor has run, you can:

- Make changes to the script and define thresholds for metrics that were created or updated in the run. For details, see Threshold Settings in the Using SiteScope Guide.
- Check status and values of the metrics in the SiteScope Dashboard.
- Set up alerts on the monitor. For details, see How to Configure an Alert in the Using SiteScope Guide.

## 11. Create a monitor template - optional

- To copy the monitor to a template, right-click the monitor, select **Copy to Template**, and select the template group to which you want to add the copied configuration. For details, see How to Create a Template by Copying Existing Configurations in the Using SiteScope Guide.
- Make any necessary changes such as adding template variables to the template. For details on template variables, see New Variable Dialog Box in the Using SiteScope Guide.

## 12. Create a content package - optional

- Copy the files used for creating the monitor to the predefined content package subfolders:
  - **<SiteScope>\packages\workspace\package\_<Package ID>\lib**. (Optional) Copy any external jars used by the custom monitor script to this folder. Java classes from the jar files can be accessed from the data processing script. Note that you can use this monitor without external jars.

**Note:** In the data processing script, to import a package from a jar that does not start with com., org., or java., you must add the package's prefix:  
importPackage(Packages.<packageName>)

For example, importPackage(Packages.it.companyname.test);

For details on importing Java classes and packages, see  
<http://www.mozilla.org/rhino/ScriptingJava.html>.

- **<SiteScope>\packages\workspace\package\_<>\classes**. (Optional) Copy the compiled Java classes with the entire package folder structure to this folder; this is not required if the class files

were packaged in a jar that was copied to the `\lib` folder. The class files can be accessed from the data processing script.

- **<SiteScope>\packages\workspace\package\_<>\conf**. (Optional) Copy the configuration files, documentation, and XML files to this folder.
- **<SiteScope>\packages\workspace\package\_<>\template**. (Optional) The folder should contain the template files exported from SiteScope (performed in ["Create a monitor template - optional" on the previous page](#)). Each template can contain various types of monitors, custom and regular.

b. Copy extension files - optional

If the monitor references script or alert extension files in the SiteScope file system, copy them to the relevant folders in **<SiteScope root directory>\packages\workspace\extensions**:

- **\scripts**. Used for storing script files that are used to run shell commands or other scripts on the machine where SiteScope is running.
- **\scripts.remote**. Used for storing script files that are used for running a script that is stored on a remote machine.
- **\templates.mail**. Used for storing the file containing the format and content of alert messages sent by email.
- **\templates.mail.subject**. Used for storing the file containing the subject line of alert messages sent by email.
- **\templates.mib**. Used for storing the MIB files that are used to create a browsable tree that contains names and descriptions of the objects found during a traversal.
- **\templates.os**. Used for storing the shell commands to be run when monitoring remote UNIX servers.

**Note:**

- On exporting the files to a content package, the unique package ID is added to the script and template files as a suffix (before the file extension) under the relevant folder in the SiteScope root directory.
- As part of the import process, the **template.os** and **templates.mib** files are edited and the unique package ID is added to some properties inside the files.

c. Export the content package to a zip file

Select the **Templates** context. In the template tree, right-click the template or template container that you want to export to a content package, and select **Export > Content Package**.

In the Export Content Package Wizard, enter details of the content package (manifest), and select the templates and files associated with these templates to include. For Wizard details, see Export Content Package Wizard.

For task details, see How to Create, Export, and Import a Custom Monitor Content Package and How to Create, Export, and Import a Template Extension Content Package in the Using SiteScope Guide.

**Note:** The Select Files page of the Wizard displays files from the **<SiteScope root directory>\packages\workspace\package\_<Package ID>** and **<SiteScope root directory>\packages\workspace\extensions** folders listed above, except for the **\META-INF** and **\templates** folders which are not displayed.

### 13. Share the custom monitor with other SiteScope users - optional

You can distribute a content package zip file by:

- Sending it to individual SiteScope users.
- Sharing it with other SiteScope users by uploading it to the Community Content for SiteScope page on [HPE Live Network](https://hpln.hpe.com/group/sitescope) (<https://hpln.hpe.com/group/sitescope>). HPE Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HPE Software portfolio.

For task details, see [How to Publish Content to the HPE Live Network Community](#).

## How to Debug a Custom Monitor Offline

This task describes the steps involved in offline debugging of a custom monitor script using a remote debugging environment. This makes the script development process easier, since it enables you to complete the code and see the debugged data inside the script during the data processing stage.

#### 1. Prerequisites

To perform offline debugging, the Eclipse IDE with Web Tools must be installed on a local machine.

#### 2. In SiteScope, enable the global custom monitor debugging setting in SiteScope Preferences

Select **Preferences > Infrastructure Preferences > Custom Monitor Settings**, and select the **Enable custom monitor debugging** check box.

#### 3. In SiteScope, create a custom monitor with offline debugging enabled

Create a custom monitor. For details, see the previous task.

When configuring the monitor settings, expand **Custom Monitor Settings**, and under the Data Processing Script section, select **Enable monitor debugging**.

Save the monitor.

#### 4. Copy the Custom Monitor Debugging Eclipse project to the debugging environment

The Custom Monitor Debugging Eclipse project is available (in zip format) from:

- **<SiteScope root directory>\examples\monitors\custom\CustomMonitorDebuggingEclipseProject**.
- The Community Content for SiteScope page on the HPE Live Network (<https://hpln.hp.com/group/community-content-sitescope>).

**Note:** Make sure you use the correct version of the Custom Monitor Debugging Eclipse project. SiteScope 11.23 is compatible with version 2.0 of the project (**SISProxy-2.0.min.js**).

#### 5. Import the Custom Monitor Debugging project into Eclipse IDE

- a. On the debugging environment, open Eclipse IDE and click **Import**.
- b. Select **General > Existing Project into Workspace**, and click **Next**.
- c. Select the Custom Monitor Debugging Eclipse project (zip file).

#### 6. Copy the SiteScope Custom Monitor Data Processing Script to the Custom Monitor Debugging project

- a. Copy the content of Data Processing Script from the SiteScope custom monitor to **MonitorScript.js** script.



- b. Connect to the SiteScope monitor by entering the following in the **DebugConfiguration.js** file:
  - **host**. Name of the SiteScope server.
  - **port**. Port used by the SiteScope server.
  - **username**. Username for accessing the SiteScope server.
  - **password**. Password to access the SiteScope server.
  - **monitorPath**. Full path to the custom monitor to debug in SiteScope including the monitor name, separated by "/". For example, Group1/Group2/Group3/Custom Monitor Name.
7. Enable the debugger to use external jar files - optional (where the script uses external jar files)  
If the monitor script uses external jar files, copy the jar files from **<SiteScope root directory>\packages\workspace\package\_<Package ID>\lib** to the **<JRE installation path>\lib\ext** directory on the debugging environment.
8. Run the debugger
  - a. In the Eclipse IDE, select **Debug Configuration**.
  - b. Select **Rhino JavaScript > Custom Monitor Debugging - MonitorScript.js**.
  - c. The debugger connects to SiteScope, and runs the script within the monitor.  
SiteScope returns the data to the debugger and then disconnects. This enables the debugger to simulate the script running the same data.
9. Debug the script  
Use Eclipse IDE to debug the script.

## How to Access the Monitor Configuration Parameters Exposed in the Script

### Data Processing Script:

- You can access the configuration parameters for custom monitors in the data processing script using:

```
myContext.getInputData().getConfigurationParameter("<configuration parameter name>");
```

Example:

```
var monitorName = myContext.getInputData().getConfigurationParameter("monitorName");
```

The following monitor properties are exposed to the script (for all custom monitors):

- `monitorName`. The name of the monitor.
- `monitorDescription`. A description of the monitor.

The following monitor properties are exposed to the script for the Custom Database monitor only:

- `dbConnectionUrl`. The connection URL of the database to which you want to connect.

- You can set the summary string which is used as the monitor status in the SiteScope Dashboard using:

```
myContext.getScriptResult().setSummary("<text summary>");
```

The default value is: `summary = <a set of metrics and their values>`

- You can set monitor availability which is displayed in the SiteScope Dashboard using:

```
myContext.getScriptResult().setAvailability(<true/false>)
```

The default value is: `availability = true`

### Topology Script:

You can access the configuration parameters for custom monitors in the topology script using:

```
Framework.getDestinationAttributeAsObject("configuration").get("<configuration parameter name>")
```

To access data saved in the monitor storage (this is a place where you can save script data for use in future executions):

```
Framework.getDestinationAttributeAsObject("monitorStorage").get("<configuration parameter name>")
```

To access the list of metric names used in the script:

```
Framework.getDestinationAttributeAsObject("metrics")
```

## How to Import and Use a Custom Database Monitor

After developing a custom monitor and creating a content package zip file, the content package can then be sent to specific users, or be published to the [HPE Live Network](https://hpln.hpe.com/group/sitescope) (<https://hpln.hpe.com/group/sitescope>) community enabling other users to import the monitor for their own use.

For details on using the Wizard, see Export Content Package Wizard.

### 1. Prerequisites

Only a SiteScope administrator user, or a user granted the **Add, edit or delete templates** permissions can import monitor templates from a content package. For details, see Permissions.

### 2. Access the custom monitor content package zip file

- If a content package zip file was sent to you, skip to the next step.
- If a content package was made available to the Community Content for SiteScope page on [HPE Live Network](https://hpln.hpe.com/group/sitescope), download the content package to your SiteScope machine. HPE Live Network is an online community providing a central location for HPE customers to share information and learn about add-on content, extensions and related activities across the HPE Software portfolio.

For task details, see How to download a template or content package from the HPE Live Network in the Using SiteScope Guide.

### 3. Import the custom monitor content package

- a. In SiteScope, select the **Templates** context. In the template tree, right-click the template container into which you want to import the content package, and click **Import**.
- b. In the Content Import dialog box, select **Content package**, and click the **Browse** button. Navigate to the folder containing the package you want to import (packages are distributed in zip format). Click **Open**, and then click **OK**. For details on the Content Import dialog box, see Content Import Dialog Box in the Using SiteScope Guide.

For task details, see How to Create, Export, and Import a Custom Monitor Content Package and How to Create, Export, and Import a Template Extension Content Package in the Using SiteScope Guide.

### 4. Verify the template was imported successfully by checking it was added to the template tree

The content package is copied to the **<SiteScope root directory>\packages\imported** folder, and a new folder is created with the name: **<Package/Zip Name>.zip\_<Package ID>**.

The folder contains:

- **\META-INF**. Contains the manifest file where information about the content package is stored.
- **\templates**. Contains files from which templates in this content package were imported into SiteScope.
- **<Package/Zip Name>**. Uncompressed package that contains the above-mentioned folders, the **\extensions** folder which contains script and alert template files referenced by monitors in the imported templates, and the folders used for Custom monitors:
  - **\classes**. Used for storing compiled Java classes.
  - **\conf** Used for storing configuration files, documentation, and XML files.
  - **\lib** Used for storing external jar files used by the monitor script. Note that the **\lib** folder is shared between all monitors imported in the same template.
- **<Package/Zip Name>.zip.properties**. This is the descriptor (manifest) file for content packages created in SiteScope 11.20, that is used in case of rollback, uninstall, or upgrade. The file contains the ID of the SiteScope template that was deployed, the location of the files in SiteScope, and other information about the content package.

The imported templates and dependency files can be used directly or modified as required.

Where script or alert templates are referenced in the user interface, the unique package ID is added as a suffix.

**Example:** ShortMail alert action template referenced in the Template field.

The screenshot shows a web-based form titled "Action Type Settings". It contains several input fields with labels and asterisks indicating required fields. The "Template" field is highlighted with a red asterisk and contains the text "ShortMail\_06b62f60-807c-4102-adea-9a7ebdd80e8b". Other fields include "Action name" (E Mail), "Recipients" (Default), "Addresses" (empty), "Subject" (Typical), and "Template" (ShortMail\_06b62f60-807c-4102-adea-9a7ebdd80e8b).

## 5. Deploy the custom monitor template

After importing the custom monitor template, you can deploy the template to a group.

- In the template tree, right-click the custom monitor 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 user interface details, see Select Group Dialog Box in the Using SiteScope Guide.
- In the Deployment Values dialog box, enter the required variable values in the entry boxes displayed, and click **OK**. The entry boxes displayed correspond to the template variables used in the template objects. For user interface details, see Deployment Values Dialog Box in the Using SiteScope Guide.

**Note:** When deploying the template or publishing changes in the template to deployed groups, clearing the **Verify monitor properties with remote server** check box in the Deployment

Values dialog box has no effect, because the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.

- d. Verify that the template was deployed successfully (the template objects should be added to the specified group in the monitor tree).

For task details, see How to Deploy Templates Using the User Interface in the Using SiteScope Guide.

## 6. Configure monitor status thresholds

When deploying the template, only the default metrics included with the monitor are displayed (custom metrics defined in the script do not exist until after the monitor has run). For example, when configuring a Custom Log File monitor, the following metrics are default: `line`, `lines/min`, `matches`, `matches/min`.

After the monitor run, you can define thresholds for metrics that were resolved in the run. In the **Threshold Settings** panel of the custom monitor, select metrics for which you want to define thresholds in the **Condition** column by using variables or free text, or selecting default metrics from the drop-down list, and enter the value applicable to the metric parameter.




# UI Descriptions



## Custom Database Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>Database connection URL</b>	<p>Connection URL of the database to which you want to connect. The syntax should be in the format:</p> <p><code>jdbc:&lt;sub protocol&gt;:&lt;subname&gt;</code> or  <code>&lt;IP address&gt;:&lt;database server port&gt;:&lt;sid&gt;</code>.</p> <p><b>Example:</b> To connect to the Oracle 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>
<b>Database driver</b>	<p>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 <b>&lt;SiteScope root directory&gt;\WEB-INF\lib\</b> directory.</p> <p><b>Default value:</b> <code>sun.jdbc.odbc.JdbcOdbcDriver</code></p> <p><b>Tip:</b> You can specify database drivers that have timeout problems (where database queries processed with these drivers exceed the timeout specified in the monitor's <b>Query timeout</b> field) in the <b>Timeout proxied query drivers list</b> field (in <b>Preferences &gt; Infrastructure Preferences &gt; General Settings</b>). These drivers are queried separately with a monitor-based timeout.</p>

UI Element	Description
<b>Database user name</b>	<p>User name used to log on to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystem JDBC-ODBC bridge driver, <code>sun.jdbc.odbc.JdbcOdbcDriver</code>), you can leave this blank and choose Windows Authentication when you setup the ODBC connection.</p> <p>With Windows 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>
<b>Database password</b>	<p>Password used to log on to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystem JDBC-ODBC bridge driver (<code>sun.jdbc.odbc.JdbcOdbcDriver</code>), you can leave this blank and choose Windows Authentication when you create the ODBC connection.</p> <p>With Windows Authentication, SiteScope connects using the login account of the SiteScope service.</p>
<b>Max rows</b>	<p>Maximum number of rows the monitor retrieves from the database for each monitor run. 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. The same rows in the amount limited by this property value are retrieved from the beginning of the table on each monitor run if <b>Enumerating field</b>, <b>Enumerating field type</b> and <b>Initial enumerating value</b> fields are not populated.</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> <p><b>Default value:</b> 5000 rows</p>
<b>Physically close if idle connection count exceeds</b>	<p>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>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>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>

UI Element	Description																			
<b>Use connection pool</b>	Enables SQL connection sharing. This means that you use a connection pool rather than open and close a new connection for each monitor query. <b>Default value:</b> Selected																			
<b>Queries</b>																				
	<b>New query.</b> Adds a new line to the Database queries table, enabling you to enter a new query.																			
	<b>Edit query.</b> Opens the Query Editor, in which the selected SQL query is displayed and can be edited.																			
	<b>Delete query.</b> Deletes the selected query.																			
<b>No</b>	The query number. By default, you can add up to 10 queries to the table. The queries are run in the order in which they appear in the table. <b>Note:</b> You can modify the number of queries that can be added to the table by changing the <b>Maximum number of queries</b> value in <b>Preferences &gt; Infrastructure Preferences &gt; Custom Monitor Settings</b> .																			
<b>Queries</b>	Enter a query for each database instance and table in the database you want to monitor. You can create or edit a query in the table (in line mode), or in the Query Editor. To open the Query Editor, click the <b>Edit query</b> button. It is recommended to use the Query Editor when adding or viewing long queries.																			
<b>Enumerating field</b>	Enumeration means the monitor retrieves the rows that were added to the queried table since its last execution. Enumerating field is the column name for the database field that the monitor uses for retrieving these rows. <b>Note:</b> The column used as enumerating field must be included in the SELECT clause.																			
<b>Enumerating field type</b>	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. The following table maps SQL types to the required enumerating field type.																			
	<table> <tr> <th>SQL Type</th><th>Enumerating Field Type</th></tr> <tr> <td>SMALLINT</td><td>INTEGER</td></tr> <tr> <td>INTEGER</td><td>INTEGER / LONG</td></tr> <tr> <td>BIGINT</td><td>LONG</td></tr> <tr> <td>NUMERIC</td><td>LONG</td></tr> <tr> <td>DOUBLE</td><td>DOUBLE</td></tr> <tr> <td>DECIMAL</td><td>DOUBLE</td></tr> <tr> <td>FLOAT</td><td>DOUBLE</td></tr> <tr> <td>TIMESTAMP</td><td>TIMESTAMP</td></tr> <tr> <td>DATE</td><td>TIMESTAMP</td></tr> </table>	SQL Type	Enumerating Field Type	SMALLINT	INTEGER	INTEGER	INTEGER / LONG	BIGINT	LONG	NUMERIC	LONG	DOUBLE	DOUBLE	DECIMAL	DOUBLE	FLOAT	DOUBLE	TIMESTAMP	TIMESTAMP	DATE
SQL Type	Enumerating Field Type																			
SMALLINT	INTEGER																			
INTEGER	INTEGER / LONG																			
BIGINT	LONG																			
NUMERIC	LONG																			
DOUBLE	DOUBLE																			
DECIMAL	DOUBLE																			
FLOAT	DOUBLE																			
TIMESTAMP	TIMESTAMP																			
DATE	TIMESTAMP																			

UI Element	Description
<b>Initial enumerating value</b>	<p>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>Script Parameters Table</b>	
	<b>Add Parameter.</b> Adds a new line to the Script Parameters table, enabling you to define parameters for use in the custom monitor script.
	<b>Delete Parameter.</b> Deletes the selected parameter.
<b>Parameter Name</b>	The name assigned to the parameter. All parameter names must be different.
<b>Parameter Value</b>	<p>The parameter value.</p> <p>If you want to hide a parameter value such as a password, select the <b>Hide Value</b> check box. The value is masked behind asterisks (*****) in the user interface.</p>
<b>Hide Value</b>	<p>Select to hide the parameter value in the Script Parameters table and in the custom monitor script. The value is masked behind asterisks (*****).</p> <p>This option is useful for an administrator in SiteScope when creating custom monitor templates, since it enables the monitor to be deployed without the parameter value being displayed in the monitor view.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> The hide option is editable when working in template mode only.</p>
<b>Configuration File</b>	Use the <b>Browse</b> button to select the configuration file. The configuration file must be a valid XML file. If it is not, then an error message is displayed. The XML configuration file is copied into the conf folder of the monitor.
<b>Data Processing Script</b>	
<b>&lt;Script&gt;</b>	<p>The input data for the data processing script is displayed in this box.</p> <p>Define the script that parses the results and creates new metrics. For details on the monitor configuration properties in the script, including how to access them, and the monitor storage and metrics names, see <a href="#">"How to Access the Monitor Configuration Parameters Exposed in the Script" on page 113</a>.</p> <p><b>Note:</b> By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the <b>Maximum number of counters</b> value in <b>Preferences &gt; Infrastructure Preferences &gt; Custom Monitor Settings</b>.</p>

UI Element	Description
<b>Package path</b>	<p>Path generated by SiteScope where the files used for developing the monitor can be saved. This enables you to add the jars on which the monitor depends (if applicable), classes, configuration, and templates files to the monitor. The path is displayed as read only.</p> <p>Click the <b>Create Path</b> button to create a folder with a relative path in the SiteScope root directory (packages\workspace\package_&lt;unique ID&gt;). The path is displayed as read only.</p> <p>The folder contains the following subfolders into which you copy the files used to create the monitor:</p> <ul style="list-style-type: none"> <li>• <b>lib.</b> (Optional) Used for storing external jar files used by the monitor script. Note that you can use this monitor without external jars.</li> <li>• <b>classes.</b> (Optional) Used for storing Java compiled classes; note that they should be copied with the entire package folder structure.</li> <li>• <b>conf.</b> (Optional) Used for storing configuration files, documentation, and XML files.</li> <li>• <b>template.</b> (Mandatory) Used for storing the template files that contain the custom monitor. It must contain at least one template. Each template can contain various types of monitors; custom and regular.</li> </ul> <p><b>Note:</b> This field is displayed when working in monitor mode only. When working in template mode and the monitor is deployed, the content pack is imported into the path.</p> <p><b>Enable monitor debugging:</b> Select the checkbox to enable sending debugging logs for custom monitors to a remote debugging server. Note that custom monitor debugging must also be enabled in <b>Infrastructure Preferences</b>. (<b>Infrastructure Preferences</b> &gt; <b>Custom Monitor Settings</b> &gt; <b>Enable custom monitor debugging</b>).</p>
<b>Checksum</b>	Click <b>Calculate Checksum</b> to calculate the MD5 checksum of a specific folder and the script.
<b>Use Tool</b> (Lower left side of the New Custom Database Monitor dialog box)	Click the <b>Use Tool</b> button to open the Database Connection tool when configuring or editing a monitor. This enables you 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). For details on the tool, see Database Connection Tool in the Using SiteScope Guide.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and limitations for the Custom Database monitor.

- ["General Tips/Limitations" on the next page](#)
- ["Custom Monitor Logs" on the next page](#)



- ["Possible Errors Using the Oracle Thin Driver" below](#)
- ["Possible Errors Using the MySQL Driver" on the next page](#)
- ["Possible Errors with Sybase Database Monitoring" on the next page](#)

## General Tips/Limitations

- If a user-defined or imported Java package has the same name as an existing SiteScope or standard Java package, SiteScope ignores the user-defined/imported Java package.
- When setting custom monitor metrics with a string (non-numeric) value, the maximum and average values in the Measurement Summary table of the Management Report are shown as 'n/a'. This also occurs if you change the metric value type, for example, if you set the metric with a numeric value, and later change it to a string value or vice versa.
- When deploying a custom monitor using a template, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, because the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.
- When publishing changes to a template that contains a custom monitor, we recommend using the **Disable custom monitors while publishing changes** option (selected by default) in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. The monitor is temporarily disabled before changes are published and is restored to the enabled state after changes have been made.
- Setting status thresholds using a baseline is not supported on user-defined metrics.
- You can use third-party .jar files without removing the JVM security from the registry by adding the `_scriptSandboxRuntimePermissions` property to the `<SiteScope root directory>\groups\master.config` file, and specifying the permitted jar files. For example, to use signed libraries `jopcagtbases.jar` and `jopcagtmessages.jar`, configure the parameter as follows: `_scriptSandboxRuntimePermissions=loadLibrary.jopcagtbases, loadLibrary.jopcagtmessages`. For the types of runtime permissions that can be used, see Runtime Permission class in the [Java API documentation](#) (<http://docs.oracle.com/javase/7/docs/api/java/lang/RuntimePermission.html>).
- If running a dynamic query from within a data processing script fails, an exception is thrown.

## Custom Monitor Logs

- Errors in the monitor (including errors in the script) are written to the SiteScope logs in the same way as for any other monitor. Check the **error.log** and **RunMonitor.log** files.
- Error messages from the script are displayed in the **custom\_monitor.log** file located in `<SiteScope root directory>\logs\custom_monitors`. This log can be used for info, warning, error, and debug messages from running the script.

To change the log level to **DEBUG** mode, in `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties`, change `$(loglevel)` to **DEBUG** in the following paragraph:

```
# Custom monitors category
log4j.category.CustomMonitor=$(loglevel),custom.monitor.appender
log4j.additivity.CustomMonitor=false change
```

## 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, Io 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, Io 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, 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 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 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 enabling SiteScope to monitor a MySQL database, you get an authorization error in the Database Query monitor, 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.
- **error, driver connect error, com/sybase/jdbc/SybDriver.** Verify there are no spaces at the end of the driver name. Save the changes and try the monitor again.
- **connect error, JZ006: Caught IOException: java.net.UnknownHostException: dbservername.** Verify the name of the database server in **Database connection URL** is correct.

# Chapter 19: Custom Log File Monitor

The Custom Log File monitor broadens the capabilities of Log File monitors which are used to automatically scan log files for error information, thereby eliminating the need to manually scan the logs. You can create your own Log File monitor that scans for matches in the form of a text phrase or regular expression, and a script that processes the collected data and creates metrics. You can use Java code developed by yourself or by a third-party to process the data.

You can share custom monitors by publishing them to the HPE Live Network community, enabling other SiteScope users to import the monitor template for their own use.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **Custom Log File** monitor.

## Learn About

This section includes:

- ["Custom Log File Monitor Overview" below](#)
- ["Scheduling the Monitor" on the next page](#)
- ["Customizing Custom Log File Content Matches and Monitor Alerts" on the next page](#)
- ["Support for IPv6 Addresses" on page 125](#)
- ["License Consumption" on page 125](#)

## Custom Log File Monitor Overview

The Custom Log File monitor enables you to develop your own Log File monitor on top of the SiteScope infrastructure.

Custom monitors enable you to do the following:

- **Create monitors that provide additional metrics not available in existing monitors**

You can define a text phrase or regular expression that watches for log file entries, and create new metrics from the collected data. Each time the monitor runs, it updates the metrics and returns a status for the metrics defined in the script.
- **Process the collected data**

The returned data can be extracted and processed in the script. For example, you can create a monitor that scans a log file for content match of **system time** and **idle time** values, and develop a script that creates a metric named **sum of overall CPU usage**, which is the sum of these values.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor API Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**).
- **Customize how results are displayed**

You can determine how results are displayed. For example, whether result data is displayed in megabytes or kilobytes.

- **Debug custom monitors offline**

You can perform offline debugging of a custom monitor script using a remote debugging server. This makes the script development process easier, since it enables you to complete the code and see the debugged data inside the script during the data processing stage. For details, see ["How to Debug a Custom Monitor Offline" on page 133](#).

After developing the monitor, you can:

- **Define thresholds for new metrics**

Because some metrics are defined only during a script run, you cannot define thresholds for them in advance. After the script has run for the first time and the metrics have been defined, you can then define thresholds for them. This provides more advanced data processing options than regular monitors. Note that metrics can change between script runs, for example, where variables are used in metric names. Thresholds using a metric that does not exist after the monitor run are removed automatically.

- **Share the monitor with other SiteScope users**

After developing the monitor, you can export the monitor to a template, add external jars and/or classes if the monitor depends on them, and create a content package. The content package can then be sent to specific users, or shared with other SiteScope users by publishing it to the SiteScope community on [HPE Live Network](https://hpln.hpe.com/group/sitescope) (<https://hpln.hpe.com/group/sitescope>).

By sharing knowledge with other SiteScope users, you can benefit from extended SiteScope monitor coverage and the development of new monitors outside the SiteScope release cycle.

## Scheduling the Monitor

You can schedule Custom 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.

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 the ["Check from beginning" on page 139](#) property.

## Customizing Custom Log File Content Matches and Monitor Alerts

You can create a Custom Log File monitor that triggers customized alerts for content matches according to the threshold status of the monitor.

**To configure the Custom Log File monitor with custom matches and alerts:**

1. In the Custom Log File 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 Custom 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 [How to Configure an Alert in the Using SiteScope Guide](#).

## Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the following protocols are supported:

- NetBIOS (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

For details on using IPv6, see [Support for IP Version 6 in the Using SiteScope Guide](#).

## License Consumption

Points-based Usage	Capacity-based Usage
One point for every 10 metrics. For example, 41 metrics consume 5 points.	One OSi license per monitored host.

## Tasks

This section includes:

- ["How to Develop the Custom Log File Monitor" below](#)
- ["How to Debug a Custom Monitor Offline" on page 133](#)
- ["How to Access the Monitor Configuration Parameters Exposed in the Script" on page 134](#)
- ["How to Import and Use a Custom Log File Monitor" on page 135](#)

## How to Develop the Custom Log File Monitor

### 1. Prerequisites

- You should be an advanced SiteScope user with knowledge of writing scripts in JavaScript, and have knowledge of the content of the log file of the application being monitored.
- The following configuration requirements must be performed or verified before the Custom 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.

## 2. Create a Custom Log File monitor with the relevant regular expressions to match lines in the log file

- a. Create a group into which you want to add the custom monitor. Right-click the group, select **New > Monitor**, and select the **Custom Log File** monitor.
- b. In the **General Settings** panel, enter a name and description for the monitor.
- c. In the **Custom Log File Monitor Settings** panel, configure the monitor properties as described in the UI Descriptions section below.

In the **Content match** box, enter a regular expression depending on whether:

- You want to process matched rows only (in which case, the regular expression should not contain groupings). For sample configuration details and results, see ["Example A - Configuring a Custom Log File monitor without grouping" below](#).
- You want to process the matched rows and custom matching values (in which case, the regular expression should contain groupings). For sample configuration details and results, see ["Example B - Configuring a Custom Log File monitor with matching custom values \(grouping\)" on the next page](#).
- You are running the monitor on a remote UNIX machine. For sample configuration details and results, see ["Example C - Configuring a Custom Log File monitor to run on a remote UNIX server" on page 128](#).

All matched lines of the log file are processed as input data for the data processing script.

### Example A - Configuring a Custom Log File monitor without grouping

- Configure the following properties in Custom Log File Monitor Settings:

**Content match:** /ERROR/

- For logs:

```
2012-05-01 13:40:17, ERROR - request failed
2012-05-01 13:41:55, INFO - system check complete
2012-05-01 13:43:08, INFO - new record created
2012-05-01 13:47:12, INFO - Starting service: Event Integration Startup Task
2012-05-01 13:47:12, INFO - Starting service: Statistics Task
2012-05-01 13:47:12, INFO - Starting service: SQL Connection Management Service
2011-09-07 16:50:43, ERROR - Standard directory handler failed with exception
2011-09-07 16:58:01, INFO - The Heartbeat Scheduler was started
```

The result is the following two lines:

```
2012-05-01 13:40:17, ERROR - request failed
2011-09-07 16:50:43, ERROR - Standard directory handler failed with exception
```

### Example B - Configuring a Custom Log File monitor with matching custom values (grouping)

- Configure the following properties in Custom Log File Monitor Settings:

**Content match:** /Used Memory=([0-9]\*)MB Available Memory=([0-9]\*)MB/

**Match value label:** used,available

- For logs:

```
2011-09-12 16:46:23,390 [StatisticsLogger]
INFO - Used Memory=56MB Available Memory=439MB Total Memory=496MB
Max Memory=496MB

2011-09-12 16:46:23,390 [StatisticsLogger]
INFO - PoolName=ProcessPool::perfex utilization=0.0%
avgWaitInQueueTime=0 poolMaxSize=200 execTime=0

2011-09-12 16:46:23,390 [StatisticsLogger]
INFO - PoolName=ProcessPool::perfex_dispatcher utilization=0.0%
avgWaitInQueueTime=0 poolMaxSize=200 execTime=0

2011-09-12 16:46:23,390 [StatisticsLogger]
INFO - executionCount=0 averageTime=?ms driftAverageTime=?ms

2011-09-12 16:47:23,382 [StatisticsLogger]
INFO - Used Memory=51MB Available Memory=444MB Total Memory=496MB
Max Memory=496MB
```

The result is the following two lines and values in bold (for the used and available labels):

```
2011-09-12 16:46:23,390 [StatisticsLogger]
INFO - Used Memory=56MB Available Memory=439MB Total Memory=496MB
Max Memory=496MB

2011-09-12 16:47:23,382 [StatisticsLogger]
INFO - Used Memory=51MB Available Memory=444MB Total Memory=496MB
Max Memory=496MB
```

### Example C - Configuring a Custom Log File monitor to run on a remote UNIX server

- Configure the following properties in Custom Log File Monitor Settings:

**Content match:** /Used Memory=([0-9]\*)MB Available Memory=([0-9]\*)MB/

**Match value label:** used,available

**Server-side processing:** Selected

**Return matching raw data from server-side:** Not selected

- For logs:

```
2011-09-12 16:46:23,390 [StatisticsLogger] INFO - Used Memory=56MB
Available Memory=439MB Total Memory=496MB Max Memory=496MB

2011-09-12 16:46:23,390 [StatisticsLogger] INFO - PoolName=ProcessPool::
perfex utilization=0.0% avgWaitInQueueTime=0 poolMaxSize=200 execTime=0

2011-09-12 16:46:23,390 [StatisticsLogger] INFO - PoolName=ProcessPool::
perfex_dispatcher utilization=0.0% avgWaitInQueueTime=0 poolMaxSize=200 execTime=0

2011-09-12 16:46:23,390 [StatisticsLogger] INFO - executionCount=0
averageTime=?ms driftAverageTime=?ms
```

```
2011-09-12 16:47:23,382 [StatisticsLogger] INFO - Used Memory=51MB
Available Memory=444MB Total Memory=496MB Max Memory=496MB
```

The result is the following two lines and values in bold (for the used and available labels):

```
2011-09-12 16:46:23,390 [StatisticsLogger] INFO - Used Memory=56MB
Available Memory=439MB Total Memory=496MB Max Memory=496MB

2011-09-12 16:47:23,382 [StatisticsLogger] INFO - Used Memory=51MB
Available Memory=444MB Total Memory=496MB Max Memory=496MB
```

### 3. Create script parameters - optional

You can create a list of parameters that can be repeatedly used in the data processing script. To do so, enter the parameter name and value in the Script Parameters Table.

For example, you might want to create a host, user name, and password parameter. You can choose to hide parameter values, such as passwords, behind asterisks (\*\*\*\*\*) in the user interface. The hide option is editable when working in template mode only.

For user interface details, see the UI Descriptions section below.

**Note:** By default, the maximum number of parameters allowed in the table is 10. When the maximum number of rows is reached, no additional rows can be added. You can modify this number by changing the **Custom monitor maximum number of script parameters** value in **Preferences > Infrastructure Preferences > Custom Settings**. You must restart SiteScope if you change this setting.

### 4. Create the data processing script

In the **Data Processing Script** area, create the script that parses raw data and log match values and creates new metrics according to the name that you determined.

For example, you could write a script that calculates sum of the **system time** and **idle time** that are transferred as a result of log file scanning. The new metric will be displayed in the SiteScope Dashboard as **sum of overall CPU usage**.



For details on the monitor configuration properties, including how to access them, and the monitor storage and metrics names, see ["How to Access the Monitor Configuration Parameters Exposed in the Script" on page 134](#).

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor API Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**). A sample jar file showing the custom monitor's capability to access Java code is provided in the **<SiteScope root directory>\examples\monitors\custom\lib** folder.

For details on scripting in Java, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

**Tip:**

- A sample Custom Log File monitor script is provided in the **Data Processing Script** box. To use it, you need to uncomment the script.
- Sample scripts for all the custom monitors are available from the sample content package located in the **<SiteScope installation directory>\examples\monitors\custom** folder. **CustomMonitorSamplePackage.zip** contains examples for SiteScope 11.20, and **CustomMonitorsExamples\_11\_21.zip** contains updated examples including a Custom Database monitor with a dynamic query, a manifest file created using the Export Content Package Wizard, and template mail and template mail subject files. To use these scripts, you need to import the custom monitor content package and then deploy the custom monitor template. For task details, see steps 3 and 4 of ["How to Import and Use a Custom Log File Monitor" on page 135](#).

**Note:**

- If your monitor needs to open a network connection to another server from the data processing script or the Java code that is called from the script, you must enable the **Allow network access** setting in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- Access for the data processing script is restricted to the following folders/files on the SiteScope server:
  - The **\conf** folder which is located inside each content package (**<SiteScope root directory>\packages\imported** or **<SiteScope root directory>\packages\workspace**) (requires *Read* permissions).
  - **<SiteScope root directory>\logs\custom\_monitors\\*** (all permissions)
- You can use the **custom\_monitor.log** file for any info, warning, error, and debug messages that you want to write during the execution of the script. The log is located in **<SiteScope root directory>\logs\custom\_monitors**. For details on changing the log to DEBUG mode, see ["Custom Monitor Logs" on page 143](#).
- By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the **Maximum number of counters** value in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- When working in template mode, you can use template variables in a data processing script.

## 5. Generate a path for storing the files used for creating the Custom Log File

## monitor

Click the **Create Path** button to create a folder where the relevant jars, classes, configuration, and template files required for running the monitor can be saved. A folder with a relative path is created under **<SiteScope root directory>\packages\workspace\package\_<Package ID>**. The path is displayed as read only.

The folder contains the following (empty) subfolders:

- **packages\workspace\package\_<>\lib**. Used for storing external jar files used by the monitor script.
- **packages\workspace\package\_<>\classes**. Used for storing compiled Java classes; note that they should be copied with the entire package folder structure.
- **packages\workspace\package\_<>\conf**. Used for storing configuration files, documentation, and XML files.
- **packages\workspace\package\_<>\template**. Used for storing the template files that contain the custom monitor (you perform this in ["Create a monitor template - optional" on the next page](#)).

You can copy the required files to these folders at this stage, or when performing ["Custom Log File Monitor" on page 123](#).

**Note:** If you add or modify jars/classes after the first monitor run, you must either:

- Restart SiteScope for the changes to take effect, or
- To avoid having to restart SiteScope, you should enable the **Reload classes and jars on each monitor run** option in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. This option should only be used during script development, and should be cleared in the production stages since it impacts performance.

### 6. Configure topology reporting - optional

To report monitor and related CI topology data to BSM's RTSM, configure the required topology reporting settings as described in [How to Configure Topology Reporting for a Custom Monitor in the Using SiteScope Guide](#).

### 7. Configure other settings for the monitor - optional

Configure other settings for the monitor as required. For details, see [Common Monitor Settings in the Using SiteScope Guide](#).

### 8. Save the monitor and wait for the first monitor run

Save the monitor. SiteScope verifies the correctness of the monitor configuration both locally and on the remote server to be monitored, before saving the settings (this is regardless of whether you clicked **Verify & Save** or **Save**).

The monitor collects data from the log files, and filters the data based on the script you supplied.

### 9. Managing custom monitors

After creating a custom monitor, you can copy, move, or delete the monitor. When doing so, this affects the content package folder (created in the **<SiteScope root directory>\packages\workspace** directory) as follows:

Action	File System Impact
Copy Monitor	Makes a copy of the content package folder in the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder.
Cut Monitor	No change.
Delete Monitor	If you delete the custom monitor, the content package folder is removed from the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder of the SiteScope file system.
Deploy template with custom monitor + content package	No change. If a deployed monitor is copied, the content package will be copied to the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder of the SiteScope file system.

## 10. Define thresholds for the metrics - optional

After the monitor has run, you can:

- Make changes to the script and define thresholds for metrics that were created or updated in the run. For details, see Threshold Settings in the Using SiteScope Guide.
- Check status and values of the metrics in the SiteScope Dashboard.
- Set up alerts on the monitor. For details, see How to Configure an Alert in the Using SiteScope Guide.

## 11. Create a monitor template - optional

- To copy the monitor to a template, right-click the monitor, select **Copy to Template**, and select the template group to which you want to add the copied configuration. For details, see How to Create a Template by Copying Existing Configurations in the Using SiteScope Guide.
- Make any necessary changes such as adding template variables to the template. For details on template variables, see New Variable Dialog Box in the Using SiteScope Guide.

## 12. Create a content package - optional

- Copy the files used for creating the monitor to the predefined content package subfolders:
  - **<SiteScope>\packages\workspace\package\_<Package ID>\lib**. (Optional) Copy any external jars used by the custom monitor script to this folder. Java classes from the jar files can be accessed from the data processing script. Note that you can use this monitor without external jars.

**Note:** In the data processing script, to import a package from a jar that does not start with com., org., or java., you must add the package's prefix:  
importPackage(Packages.<packageName>)

For example, importPackage(Packages.it.companyname.test);

For details on importing Java classes and packages, see  
<http://www.mozilla.org/rhino/ScriptingJava.html>.

- **<SiteScope>\packages\workspace\package\_<>\classes**. (Optional) Copy the compiled Java classes with the entire package folder structure to this folder; this is not required if the class files

were packaged in a jar that was copied to the `\lib` folder. The class files can be accessed from the data processing script.

- **<SiteScope>\packages\workspace\package\_<>\conf**. (Optional) Copy the configuration files, documentation, and XML files to this folder.
- **<SiteScope>\packages\workspace\package\_<>\template**. (Optional) The folder should contain the template files exported from SiteScope (performed in ["Create a monitor template - optional" on the previous page](#)). Each template can contain various types of monitors, custom and regular.

b. Copy extension files - optional

If the monitor references script or alert extension files in the SiteScope file system, copy them to the relevant folders in **<SiteScope root directory>\packages\workspace\extensions**:

- **\scripts**. Used for storing script files that are used to run shell commands or other scripts on the machine where SiteScope is running.
- **\scripts.remote**. Used for storing script files that are used for running a script that is stored on a remote machine.
- **\templates.mail**. Used for storing the file containing the format and content of alert messages sent by email.
- **\templates.mail.subject**. Used for storing the file containing the subject line of alert messages sent by email.
- **\templates.mib**. Used for storing the MIB files that are used to create a browsable tree that contains names and descriptions of the objects found during a traversal.
- **\templates.os**. Used for storing the shell commands to be run when monitoring remote UNIX servers.

**Note:**

- On exporting the files to a content package, the unique package ID is added to the script and template files as a suffix (before the file extension) under the relevant folder in the SiteScope root directory.
- As part of the import process, the **template.os** and **templates.mib** files are edited and the unique package ID is added to some properties inside the files.

c. Export the content package to a zip file

Select the **Templates** context. In the template tree, right-click the template or template container that you want to export to a content package, and select **Export > Content Package**.

In the Export Content Package Wizard, enter details of the content package (manifest), and select the templates and files associated with these templates to include. For Wizard details, see Export Content Package Wizard.

For task details, see How to Create, Export, and Import a Custom Monitor Content Package and How to Create, Export, and Import a Template Extension Content Package in the Using SiteScope Guide.

**Note:** The Select Files page of the Wizard displays files from the **<SiteScope root directory>\packages\workspace\package\_<Package ID>** and **<SiteScope root directory>\packages\workspace\extensions** folders listed above, except for the **\META-INF** and **\templates** folders which are not displayed.

### 13. Share the custom monitor with other SiteScope users - optional

You can distribute a content package zip file by:

- Sending it to individual SiteScope users.
- Sharing it with other SiteScope users by uploading it to the Community Content for SiteScope page on [HPE Live Network](https://hpln.hpe.com/group/sitescope) (<https://hpln.hpe.com/group/sitescope>). HPE Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HPE Software portfolio.

For task details, see [How to Publish Content to the HPE Live Network Community](#).

### How to Debug a Custom Monitor Offline

This task describes the steps involved in offline debugging of a custom monitor script using a remote debugging environment. This makes the script development process easier, since it enables you to complete the code and see the debugged data inside the script during the data processing stage.

#### 1. Prerequisites

To perform offline debugging, the Eclipse IDE with Web Tools must be installed on a local machine.

#### 2. In SiteScope, enable the global custom monitor debugging setting in SiteScope Preferences

Select **Preferences > Infrastructure Preferences > Custom Monitor Settings**, and select the **Enable custom monitor debugging** check box.

#### 3. In SiteScope, create a custom monitor with offline debugging enabled

Create a custom monitor. For details, see the previous task.

When configuring the monitor settings, expand **Custom Monitor Settings**, and under the Data Processing Script section, select **Enable monitor debugging**.

Save the monitor.

#### 4. Copy the Custom Monitor Debugging Eclipse project to the debugging environment

The Custom Monitor Debugging Eclipse project is available (in zip format) from:

- **<SiteScope root directory>\examples\monitors\custom\CustomMonitorDebuggingEclipseProject**.
- The Community Content for SiteScope page on the HPE Live Network (<https://hpln.hp.com/group/community-content-sitescope>).

**Note:** Make sure you use the correct version of the Custom Monitor Debugging Eclipse project. SiteScope 11.23 is compatible with version 2.0 of the project (**SISProxy-2.0.min.js**).

#### 5. Import the Custom Monitor Debugging project into Eclipse IDE

- a. On the debugging environment, open Eclipse IDE and click **Import**.
- b. Select **General > Existing Project into Workspace**, and click **Next**.
- c. Select the Custom Monitor Debugging Eclipse project (zip file).

#### 6. Copy the SiteScope Custom Monitor Data Processing Script to the Custom Monitor Debugging project

- a. Copy the content of Data Processing Script from the SiteScope custom monitor to **MonitorScript.js** script.

- b. Connect to the SiteScope monitor by entering the following in the **DebugConfiguration.js** file:
  - **host**. Name of the SiteScope server.
  - **port**. Port used by the SiteScope server.
  - **username**. Username for accessing the SiteScope server.
  - **password**. Password to access the SiteScope server.
  - **monitorPath**. Full path to the custom monitor to debug in SiteScope including the monitor name, separated by "/". For example, Group1/Group2/Group3/Custom Monitor Name.
7. Enable the debugger to use external jar files - optional (where the script uses external jar files)  
If the monitor script uses external jar files, copy the jar files from **<SiteScope root directory>\packages\workspace\package\_<Package ID>\lib** to the **<JRE installation path>\lib\ext** directory on the debugging environment.
8. Run the debugger
  - a. In the Eclipse IDE, select **Debug Configuration**.
  - b. Select **Rhino JavaScript > Custom Monitor Debugging - MonitorScript.js**.
  - c. The debugger connects to SiteScope, and runs the script within the monitor.  
SiteScope returns the data to the debugger and then disconnects. This enables the debugger to simulate the script running the same data.
9. Debug the script  
Use Eclipse IDE to debug the script.

## How to Access the Monitor Configuration Parameters Exposed in the Script

### Data Script:

- You can access the configuration parameters for custom monitors in the data script using:

```
myContext.getInputData().getConfigurationParameter(<config param name>);
```

Example:

```
var monitorName = myContext.getInputData().getConfigurationParameter("monitorName");
```

The following monitor properties are exposed to the script (for all custom monitors):

- `monitorName`. The name of the monitor.
- `monitorDescription`. A description of the monitor.

The following monitor properties are exposed to the script for the Custom Log File monitor only:

- `server`. The name of the server where the log file you want to monitor is located.
- `logFilePath`. The path of the monitor's log file.

- You can set the summary string which is used as the monitor status in the SiteScope Dashboard using:

```
myContext.getScriptResult().setSummary(<user's text summary>);
```

The default value is: `summary = <a set of metrics and their values>`

- You can set monitor availability which is displayed in the SiteScope Dashboard using:

```
myContext.getScriptResult().setAvailability(<true/false>)
```

The default value is: `availability = true`

### Topology Script:

You can access the configuration parameters for custom monitors in the topology script using:

```
Framework.getDestinationAttributeAsObject("configuration").get("<configuration parameter name>")
```

To access data saved in the monitor storage (this is a place where you can save script data for use in future executions):

```
Framework.getDestinationAttributeAsObject("monitorStorage").get("<configuration parameter name>")
```

To access the list of metric names used in the script:

```
Framework.getDestinationAttributeAsObject("metrics")
```

## How to Import and Use a Custom Log File Monitor

After developing a custom monitor and creating a content package zip file, the content package can then be sent to specific users, or be published to the [HPE Live Network](https://hpln.hpe.com/group/sitescope) (<https://hpln.hpe.com/group/sitescope>) community enabling other users to import the monitor for their own use.

For details on using the Wizard, see Export Content Package Wizard.

### 1. Prerequisites

Only a SiteScope administrator user, or a user granted the **Add, edit or delete templates** permissions can import monitor templates from a content package. For details, see Permissions.

### 2. Access the content package zip file

- If a content package zip file was sent to you, skip to the next step.
- If a content package was made available to the Community Content for SiteScope page on [HPE Live Network](https://hpln.hpe.com/group/sitescope), download the content package to your SiteScope machine. HPE Live Network is an online community providing a central location for HPE customers to share information and learn about add-on content, extensions and related activities across the HPE Software portfolio.

For task details, see How to download a template or content package from the HPE Live Network in the Using SiteScope Guide.

### 3. Import the custom monitor content package

- a. In SiteScope, select the **Templates** context. In the template tree, right-click the template container into which you want to import the content package, and click **Import**.
- b. In the Content Import dialog box, select **Content package**, and click the **Browse** button. Navigate to the folder containing the package you want to import (packages are distributed in zip format). Click **Open**, and then click **OK**. For details on the Content Import dialog box, see Content Import Dialog Box in the Using SiteScope Guide.

For task details, see How to Create, Export, and Import a Custom Monitor Content Package and How to Create, Export, and Import a Template Extension Content Package in the Using SiteScope Guide.

### 4. Verify the template was imported successfully by checking it was added to the template tree

The content package is copied to the **<SiteScope root directory>\packages\imported** folder, and a new folder is created with the name: **<Package/Zip Name>.zip\_<Package ID>**.

The folder contains:

- **\META-INF**. Contains the manifest file where information about the content package is stored.
- **\templates**. Contains files from which templates in this content package were imported into SiteScope.
- **<Package/Zip Name>**. Uncompressed package that contains the above-mentioned folders, the **\extensions** folder which contains script and alert template files referenced by monitors in the imported templates, and the folders used for Custom monitors:
  - **\classes**. Used for storing compiled Java classes.
  - **\conf** Used for storing configuration files, documentation, and XML files.
  - **\lib** Used for storing external jar files used by the monitor script. Note that the **\lib** folder is shared between all monitors imported in the same template.
- **<Package/Zip Name>.zip.properties**. This is the descriptor (manifest) file for content packages created in SiteScope 11.20, that is used in case of rollback, uninstall, or upgrade. The file contains the ID of the SiteScope template that was deployed, the location of the files in SiteScope, and other information about the content package.

The imported templates and dependency files can be used directly or modified as required.

Where script or alert templates are referenced in the user interface, the unique package ID is added as a suffix.

**Example:** ShortMail alert action template referenced in the Template field.

The screenshot shows a web-based form titled "Action Type Settings". It contains several input fields with labels and asterisks indicating required fields. The "Template" field is highlighted with a black border and contains the text "ShortMail\_06b62f60-807c-4102-adea-9a7ebdd80e8b".

Action Type Settings	
Action name:	E Mail
* Recipients:	Default
Addresses:	
* Subject:	Typical
* Template:	ShortMail_06b62f60-807c-4102-adea-9a7ebdd80e8b

## 5. Deploy the custom monitor template

After importing the custom monitor template, you can deploy the template to a group.

- In the template tree, right-click the custom monitor 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 user interface details, see Select Group Dialog Box in the Using SiteScope Guide.
- In the Deployment Values dialog box, enter the required variable values in the entry boxes displayed, and click **OK**. The entry boxes displayed correspond to the template variables used in the template objects. For user interface details, see Deployment Values Dialog Box in the Using SiteScope Guide.

**Note:** When deploying the template or publishing changes in the template to deployed groups, clearing the **Verify monitor properties with remote server** check box in the Deployment



Values dialog box has no effect, because the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.

- d. Verify that the template was deployed successfully (the template objects should be added to the specified group in the monitor tree).

For task details, see *How to Deploy Templates Using the User Interface* in the *Using SiteScope Guide*.

## 6. Configure monitor status thresholds

When deploying the template, only the default metrics included with the monitor are displayed (custom metrics defined in the script do not exist until after the monitor has run).

After the monitor run, you can define thresholds for metrics that were resolved in the run. In the **Threshold Settings** panel of the custom monitor, select metrics for which you want to define thresholds in the **Condition** column by using variables or free text, or selecting default metrics from the drop-down list, and enter the value applicable to the metric parameter.

# UI Descriptions

## Custom Log File Monitor Settings



User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>Server</b>	<p>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 Windows domain, use the UNC format to specify the path to the remote log file. For example, \\lab_machine\users\SiteScopes\Version_11.2\Build_2000\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> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

UI Element	Description
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Log file path</b>	<p>Path to the log file you want to monitor.</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 the UNIX user account being used to log on to the remote machine.</li> <li>• <b>Remote Windows through NetBIOS.</b> For reading log files on remote Windows 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>• <b>Remote Windows through SSH.</b> For reading log files on remote Windows 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</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 in the Using SiteScope Guide.</p>

UI Element	Description
<b>Run alerts</b>	<p>Method for running alerts for this monitor.</p> <ul style="list-style-type: none"> <li>• <b>For each log entry matched.</b> The monitor triggers alerts according to thresholds applied to each matching entry found. Since status can change according to thresholds for each matched entry, each alert action could be triggered many times within a monitor run.</li> </ul> <p><b>Example:</b> If you want to send a warning alert on matched text value "power off" and an error alert if more than one server is turned off, set the following thresholds:</p> <ul style="list-style-type: none"> <li>• <code>Error if matchCount &gt; 1</code></li> <li>• <code>Warning if value == 'power off'</code></li> </ul> <p>To send an error alert if only one threshold is matched, set <code>Error if value == 'power off'</code>.</p> <p>For details on how to create a Custom Log File monitor that triggers customized alerts for content matches, see <a href="#">"Customizing Custom Log File Content Matches and Monitor Alerts" on page 124</a>.</p> <ul style="list-style-type: none"> <li>• <b>Once, after all log entries have been checked.</b> 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 metric, an alert is not triggered.</p>
<b>Check from beginning</b>	<p>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>
<b>Content match</b>	<p>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 Custom 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 <code>s</code> search modifier to the end of the regular expression. For details, see Regular Expressions Overview in the Using SiteScope Guide.</p>
<b>Open Tool</b>	<p>Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.</p>
<b>Advanced Settings</b>	

UI Element	Description
<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 the 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>
<b>Rules file path</b>	<p>Enter the full path to your rules file. In special cases, it may be necessary to create a custom rules file to specify different alerts for different log entry matches. You can also set a parameter in the rules file to run script alerts. You can use any of the properties in the SiteScope Alert Template and Event Properties Directory.</p> <p>An example rules file is located in <b>&lt;SiteScope root directory&gt;\examples\log_monitor\sample.rules</b>. For instructions on how to use the file and example rules, see <a href="#">"How to Use the Rules File" on page 352</a>, or read the instructions in the file itself.</p>
<b>Match value labels</b>	<p>Use 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 Data Processing Script. Separate multiple labels with a comma (,).</p> <p><b>Note:</b> If match value labels are not used, the matched values are named <code>value1</code>, <code>value2</code>, and so forth.</p>
<b>Multi-line match</b>	<p>Runs a regular expression match on multiple lines of text.</p> <p><b>Default value:</b> Not selected</p>
<b>Server-side processing</b>	<p>Processes 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 available for remote Linux, Red Hat Enterprise Linux, and Oracle 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>Return matching raw data from server-side</b>	<p>Returns the whole row of raw data with matching patterns from the server-side when a match is found.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> This setting is only available when <b>Server-side processing</b> is selected.</p>

UI Element	Description
<b>No error if file not found</b>	Monitor remains in Good status if the file is not found. The monitor status remains Good regardless of the monitor threshold configuration. <b>Default value:</b> Not selected
<b>Timeout Settings</b>	
<b>Enable timeout</b>	The monitor stops its run after the specified timeout period has been exceeded. <b>Default value:</b> Not selected
<b>After timeout, resume reading from end of file</b>	If selected, the monitor resumes reading from the end of the log file during the next run, instead of from the current location. <b>Default value:</b> Not selected <b>Note:</b> This setting is only available when <b>Enable timeout</b> is selected.
<b>Status after timeout</b>	The status condition that the monitor goes into if the monitor times out. The status categories include: Error, Warning, Good <b>Default value:</b> Warning <b>Note:</b> This setting is only available when <b>Enable timeout</b> is selected.
<b>Timeout (seconds)</b>	Amount of time, in seconds, that SiteScope should wait before the monitor times out. <b>Default value:</b> 60 seconds <b>Note:</b> This setting is only available when <b>Enable timeout</b> is selected.
<b>Script Parameters Table</b>	
	<b>Add Parameter.</b> Adds a new line to the Script Parameters table, enabling you to define parameters for use in the custom monitor script.
	<b>Delete Parameter.</b> Deletes the selected parameter.
<b>Parameter Name</b>	The name assigned to the parameter. All parameter names must be different.
<b>Parameter Value</b>	The parameter value. If you want to hide a parameter value such as a password, select the <b>Hide Value</b> check box. The value is masked behind asterisks (*****) in the user interface.
<b>Hide Value</b>	Select to hide the parameter value in the Script Parameters table and in the custom monitor script. The value is masked behind asterisks (*****).  This option is useful for an administrator in SiteScope when creating custom monitor templates, since it enables the monitor to be deployed without the parameter value being displayed in the monitor view. <b>Default value:</b> Not selected <b>Note:</b> The hide option is editable when working in template mode only.

UI Element	Description
<b>Configuration File</b>	Use the <b>Browse</b> button to select the configuration file. The configuration file must be a valid XML file. If it is not, then an error message is displayed. The XML configuration file is copied into the <code>conf</code> folder of the monitor.
<b>Data Processing Script</b>	
<b>&lt;Script&gt;</b>	<p>The input data for the data processing script is displayed in this box.</p> <p>Define the script that parses the results and creates new metrics. For details on the monitor configuration properties in the script, including how to access them, and the monitor storage and metrics names, see <a href="#">"How to Access the Monitor Configuration Parameters Exposed in the Script" on page 134</a>.</p> <p><b>Note:</b> By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the <b>Maximum number of counters</b> value in <b>Preferences &gt; Infrastructure Preferences &gt; Custom Monitor Settings</b>.</p>
<b>Package path</b>	<p>Path generated by SiteScope where the files used for developing the monitor can be saved. This enables you to add the jars on which the monitor depends (if applicable), classes, configuration, and templates files to the monitor. The path is displayed as read only.</p> <p>Click the <b>Create Path</b> button to create a folder with a relative path in the SiteScope root directory (<code>packages\workspace\package_&lt;unique ID&gt;</code>). The path is displayed as read only.</p> <p>The folder contains the following subfolders into which you copy the files used to create the monitor:</p> <ul style="list-style-type: none"> <li>• <b>lib.</b> (Optional) Used for storing external jar files used by the monitor script. Note that you can use this monitor without external jars.</li> <li>• <b>classes.</b> (Optional) Used for storing Java compiled classes; note that they should be copied with the entire package folder structure.</li> <li>• <b>conf.</b> (Optional) Used for storing configuration files, documentation, and XML files.</li> <li>• <b>template.</b> (Mandatory) Used for storing the template files that contain the custom monitor. It must contain at least one template. Each template can contain various types of monitors; custom and regular.</li> </ul> <p><b>Note:</b> This field is displayed when working in monitor mode only. When working in template mode and the monitor is deployed, the content pack is imported into the path.</p> <p><b>Enable monitor debugging:</b> Select the checkbox to enable sending debugging logs for custom monitors to a remote debugging server. Note that custom monitor debugging must also be enabled in <b>Infrastructure Preferences</b>. (<b>Infrastructure Preferences &gt; Custom Monitor Settings &gt; Enable custom monitor debugging</b>).</p>
<b>Checksum</b>	Click <b>Calculate Checksum</b> to calculate the MD5 checksum of a specific folder and the script.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and limitations for the Custom Log File monitor.

- ["General Tips/Limitations" below](#)
- ["Custom Monitor Logs" below](#)

### General Tips/Limitations

- If a user-defined or imported Java package has the same name as an existing SiteScope or standard Java package, SiteScope ignores the user-defined/imported Java package.
- When setting custom monitor metrics with a string (non-numeric) value, the maximum and average values in the Measurement Summary table of the Management Report are shown as 'n/a'. This also occurs if you change the metric value type, for example, if you set the metric with a numeric value, and later change it to a string value or vice versa.
- When deploying a custom monitor using a template, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, because the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.
- When publishing changes to a template that contains a custom monitor, we recommend using the **Disable custom monitors while publishing changes** option (selected by default) in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. The monitor is temporarily disabled before changes are published and is restored to the enabled state after changes have been made.
- Setting status thresholds using a baseline is not supported on user-defined metrics.
- You can use third-party .jar files without removing the JVM security from the registry by adding the `_scriptSandboxRuntimePermissions` property to the `<SiteScope root directory>\groups\master.config` file, and specifying the permitted jar files. For example, to use signed libraries `jopcagtbase.jar` and `jopcagtmsg.jar`, configure the parameter as follows: `_scriptSandboxRuntimePermissions=loadLibrary.jopcagtbase, loadLibrary.jopcagtmsg`.  
For the types of runtime permissions that can be used, see Runtime Permission class in the [Java API documentation](http://docs.oracle.com/javase/7/docs/api/java/lang/RuntimePermission.html) (<http://docs.oracle.com/javase/7/docs/api/java/lang/RuntimePermission.html>).
- This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see ["How to Configure the HP NonStop Resources Monitor" on page 307](#).
- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When monitoring a log file on a FreeBSD remote server, make sure the correct path to the "cat" command is used in `<SiteScope root directory>\templates.os\FreeBSD.config`, since the command was moved in the latest FreeBSD versions.

### Custom Monitor Logs

- Errors in the monitor (including errors in the script) are written to the SiteScope logs in the same way as for any other monitor. Check the **error.log** and **RunMonitor.log** files.
- Error messages from the script are displayed in the **custom\_monitor.log** file located in `<SiteScope root directory>\logs\custom_monitors`. This log can be used for info, warning, error, and debug messages

from running the script.

To change the log level to **DEBUG** mode, in **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties**, change **\${loglevel}** to **DEBUG** in the following paragraph:

# Custom monitors category

log4j.category.CustomMonitor=**\${loglevel}**,custom.monitor.appender

log4j.additivity.CustomMonitor=false change



# Chapter 20: Custom WMI Monitor

The Custom WMI monitor broadens the capabilities of monitors that support the Windows Management Instrumentation (WMI) method for collecting data by checking the availability and performance of management data on Windows-based operating systems. You can create your own WMI monitor by developing WMI Query Language (WQL) queries that collect data, and a script that processes the collected data and creates metrics. You can use Java code developed by yourself or by a third-party to process the data.

You can share custom monitors by publishing them to the HPE Live Network community, enabling other SiteScope users to import the monitor template for their own use.

**Tip:** You can view guided and narrated demonstrations for using the WMI Custom monitor on YouTube:

- Custom WMI Monitor Creation Process and Packaging - <http://www.youtube.com/watch?v=bB6NITGdd88>
- Custom WMI Monitor Data Processing Script - <http://www.youtube.com/watch?v=Glw3JVnunWE>

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **Custom WMI** monitor.

## Learn About

### Custom WMI Monitor Overview

The Custom WMI monitor enables you to develop your own monitors on top of the SiteScope infrastructure. This provides you with greater flexibility not available in existing monitors.

You can use the Custom WMI monitor to:

- **Collect any WMI data you like**

You can create a series of pre-defined WQL queries for the Windows operating systems you want to monitor. SiteScope runs the queries and returns the results to the monitor in an object that contains a set of results for each query. Each time the monitor runs, it re-runs your queries and collects fresh data.

- **Process the collected data**

You can create a script in the monitor that can extract and process the results of the collected data. For example, you can define metrics based on collected data from the Windows operating system or perform mathematical operations on it as in the sample script provided.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor API Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**).

- **Collect data dynamically**

You can include dynamically-defined queries in the data processing script. These queries are executed while the script is running, in contrast to predefined queries, which are executed before the script is run. Dynamically-executed queries provide the added benefit of enabling you to create queries based on values

that are not in the monitored entity data store (for example, timestamp), create queries based on previous query results or calculations, and include variables in queries. For details, see [Data Processing Script with Dynamic Queries in the Using SiteScope Guide](#).

- **Debug custom monitors offline**

You can perform offline debugging of a custom monitor script using a remote debugging server. This makes the script development process easier, since it enables you to complete the code and see the debugged data inside the script during the data processing stage. For details, see ["How to Debug a Custom Monitor Offline" on page 152](#).

After developing the monitor, you can:

- **Define thresholds for new metrics**

Because some metrics are defined only during a script run, you cannot define thresholds for them in advance. After the script has run for the first time and the metrics have been defined, you can then define thresholds for them. This provides more advanced data processing options than regular monitors. Note that metrics can change between script runs, for example, where variables are used in metric names. Thresholds using a metric that does not exist after the monitor run are removed automatically.

- **Share the monitor with other SiteScope users**

After developing the monitor, you can export the monitor to a template, add external jars and/or classes if the monitor depends on them, and create a content package. The content package can then be sent to specific users, or shared with other SiteScope users by publishing it to the SiteScope community on [HPE Live Network](#) (<https://hpln.hpe.com/group/sitescope>).

By sharing knowledge with other SiteScope users, you can benefit from extended SiteScope monitor coverage and the development of new monitors outside the SiteScope release cycle.

## License Consumption

Points-based Usage	Capacity-based Usage
1 point for every 10 metrics. For example, 41 metrics consume 5 points.	One OSi license per monitored host

## Tasks

This section includes:

- ["How to Develop the Custom WMI Monitor" below](#)
- ["How to Debug a Custom Monitor Offline" on page 152](#)
- ["How to Access the Monitor Configuration Parameters Exposed in the Script" on page 153](#)
- ["How to Import and Use a Custom WMI Monitor" on page 154](#)

## How to Develop the Custom WMI Monitor

### 1. Prerequisites

- You should be an advanced SiteScope user with knowledge of writing scripts in JavaScript, and have knowledge of WMI and WQL.
- 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, 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 defined for the WMI remote server must have permissions to read statistics remotely from any name space that they use in the queries. For details, refer to <http://support.microsoft.com/kb/295292>.

For information about troubleshooting WMI service problems, see "[Tips/Troubleshooting](#)" on [page 159](#).

## 2. Create a Custom WMI monitor with the relevant queries

- a. Create a group into which you want to add the custom monitor. Right-click the group, select **New > Monitor**, and select the **Custom WMI** monitor.
- b. In the **General Settings** panel, enter a name and description for the monitor.
- c. In the **Custom WMI Monitor Settings** panel, select the server that you want to monitor (only those Windows remote servers configured with a WMI connection are available).
- d. In the WMI Queries Table, enter the WQL queries and the WMI namespace on which you want to perform the queries.

**Tip:** By default, you can enter up to 10 queries in the table. You can modify the number of queries that can be added to the table in **Preferences > Infrastructure Preferences > Custom Monitor Settings** by configuring the **Maximum number of queries** value.

For user interface details, see the UI Descriptions section below.

### Example

These queries collect processor performance and memory data from the monitored server.

No.	Queries	Namespace
0	Select PercentProcessorTime, Timestamp_Sys100NS From Win32_PerfRawData_PerfOS_Processor	root\cimv2
1	Select PercentProcessorTime, Timestamp_Sys100NS From Win32_PerfRawData_PerfOS_Processor	root\cimv2

## 3. Create script parameters - optional

You can create a list of parameters that can be repeatedly used in the data processing script. To do so, enter the parameter name and value in the Script Parameters Table.

For example, you might want to create a host, user name, and password parameter. You can choose to hide parameter values, such as passwords, behind asterisks (\*\*\*\*\*) in the user interface. The hide option is editable when working in template mode only.

For user interface details, see the UI Descriptions section below.

**Note:** By default, the maximum number of parameters allowed in the table is 10. When the maximum number of rows is reached, no additional rows can be added. You can modify this number by changing the **Custom monitor maximum number of script parameters** value in **Preferences**

> **Infrastructure Preferences > Custom Settings**. You must restart SiteScope if you change this setting.

#### 4. Create the data processing script

In the **Data Processing Script** area of Custom WMI Monitor Settings, create the script that parses the results and creates new metrics according to the name that you determined.

In addition, you can include any number of queries in the script. The queries are executed as the script is run, which means that the monitor collects fresh data from the Windows operating system being monitored. After the data is retrieved, it becomes available for the script to use. A query in a script has the same syntax as a query defined in the queries table, but it can be structured using variables which makes it dynamic within the monitor run context. For details on dynamic queries, see Data Processing Script with Dynamic Queries in the Using SiteScope Guide.

For details on the monitor configuration properties, including how to access them, and the monitor storage and metrics names, see "[How to Access the Monitor Configuration Parameters Exposed in the Script](#)" on page 153.

For details on the methods and classes that are available in the script, see the HP SiteScope Custom Monitor API Reference (available from **<SiteScope installation directory>\examples\monitors\custom\doc\javadoc.zip**). A sample jar file showing the custom monitor's capability to access Java code is provided in the **<SiteScope root directory>\examples\monitors\custom\lib** folder.

For details on scripting in Java, see <http://www.mozilla.org/rhino/ScriptingJava.html>.

##### Tip:

- A sample Custom WMI monitor script is provided in the **Data Processing Script** box. To use it, you need to uncomment the script.
- Sample scripts for all the custom monitors are available from the sample content package located in the **<SiteScope installation directory>\examples\monitors\custom** folder. **CustomMonitorSamplePackage.zip** contains examples for SiteScope 11.20, and **CustomMonitorsExamples\_11\_21.zip** contains updated examples including a Custom Database monitor with a dynamic query, a manifest file created using the Export Content Package Wizard, and template mail and template mail subject files. To use these scripts, you need to import the custom monitor content package and then deploy the custom monitor template. For task details, see steps 3 and 4 of "[How to Import and Use a Custom WMI Monitor](#)" on page 154.

##### Note:

- If your monitor needs to open a network connection to another server from the data processing script or the Java code that is called from the script, you must enable the **Allow network access** setting in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- Access for the data processing script is restricted to the following folders/files on the SiteScope server:
  - The **\conf** folder which is located inside each content package (**<SiteScope root directory>\packages\imported** or **<SiteScope root directory>\packages\workspace**)

(requires *Read* permissions).

- **<SiteScope root directory>\logs\custom\_monitors\\*** (all permissions)
- You can use the **custom\_monitor.log** file for any info, warning, error, and debug messages that you want to write during the execution of the script. The log is located in **<SiteScope root directory>\logs\custom\_monitors**. For details on changing the log to DEBUG mode, see ["Custom Monitor Logs" on page 160](#).
- By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the **Maximum number of counters** value in **Preferences > Infrastructure Preferences > Custom Monitor Settings**.
- When working in template mode, you can use template variables in a data processing script.

## 5. Generate a path for storing the files used for creating the Custom WMI monitor

Click the **Create Path** button to create a folder where the relevant jars, classes, configuration, and template files required for running the monitor can be saved. A folder with a relative path is created under **<SiteScope root directory>\packages\workspace\package\_<Package ID>**. The path is displayed as read only.

The folder contains the following (empty) subfolders:

- **packages\workspace\package\_<>\lib**. Used for storing external jar files used by the monitor script.
- **packages\workspace\package\_<>\classes**. Used for storing compiled Java classes; note that they should be copied with the entire package folder structure.
- **packages\workspace\package\_<>\conf**. Used for storing configuration files, documentation, and XML files.
- **packages\workspace\package\_<>\template**. Used for storing the template files that contain the custom monitor (you perform this in ["Custom WMI Monitor" on page 145](#)).

You can copy the required files to these folders at this stage, or when performing ["Custom WMI Monitor" on page 145](#).

**Note:** If you add or modify jars/classes after the first monitor run, you must either:

- Restart SiteScope for the changes to take effect, or
- To avoid having to restart SiteScope, you should enable the **Reload classes and jars on each monitor run** option in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. This option should only be used during script development, and should be cleared in the production stages since it impacts performance.

## 6. Configure topology reporting - optional

To report monitor and related CI topology data to BSM's RTSM, configure the required topology reporting settings as described in [How to Configure Topology Reporting for a Custom Monitor in the Using SiteScope Guide](#).

## 7. Configure other settings for the monitor - optional

Configure other settings for the monitor as required. For details, see Common Monitor Settings in the Using SiteScope Guide.

## 8. Save the monitor and wait for the first monitor run

Save the monitor. SiteScope verifies the correctness of the monitor configuration locally and on the remote server to be monitored, before saving the settings, regardless of whether you click the **Verify & Save** or **Save** button.

The monitor collects data from the Windows operating system, and filters the data based on the script you supplied.

## 9. Managing custom monitors

After creating a custom monitor, you can copy, move, or delete the monitor. When doing so, this affects the content package folder (created in the **<SiteScope root directory>\packages\workspace** directory) as follows:

Action	File System Impact
Copy Monitor	Makes a copy of the content package folder in the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder.
Cut Monitor	No change.
Delete Monitor	If you delete the custom monitor, the content package folder is removed from the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder of the SiteScope file system.
Deploy template with custom monitor + content package	No change. If a deployed monitor is copied, the content package will be copied to the <b>&lt;SiteScope root directory&gt;\packages\workspace</b> folder of the SiteScope file system.

## 10. Define thresholds for the metrics - optional

After the monitor has run, you can:

- Make changes to the script and define thresholds for metrics that were created or updated in the run. For details, see Threshold Settings in the Using SiteScope Guide.
- Check status and values of the metrics in the SiteScope Dashboard.
- Set up alerts on the monitor. For details, see How to Configure an Alert in the Using SiteScope Guide.

## 11. Create a monitor template - optional

- a. To copy the monitor to a template, right-click the monitor, select **Copy to Template**, and select the template group to which you want to add the copied configuration. For details, see How to Create a Template by Copying Existing Configurations in the Using SiteScope Guide.
- b. Make any necessary changes such as adding template variables to the template. For details on template variables, see New Variable Dialog Box in the Using SiteScope Guide.

## 12. Create a content package - optional

- a. Copy the files used for creating the monitor to the predefined content package subfolders:

- **<SiteScope>\packages\workspace\package\_<Package ID>\lib.** (Optional) Copy any external jars used by the custom monitor script to this folder. Java classes from the jar files can be accessed from the data processing script. Note that you can use this monitor without external jars.

**Note:** In the data processing script, to import a package from a jar that does not start with com., org., or java., you must add the package's prefix:

```
importPackage(Packages.<packageName>)
```

For example, `importPackage(Packages.it.companyname.test);`

For details on importing Java classes and packages, see

<http://www.mozilla.org/rhino/ScriptingJava.html>.

- **<SiteScope>\packages\workspace\package\_<>\classes.** (Optional) Copy the compiled Java classes with the entire package folder structure to this folder; this is not required if the class files were packaged in a jar that was copied to the \lib folder. The class files can be accessed from the data processing script.
  - **<SiteScope>\packages\workspace\package\_<>\conf.** (Optional) Copy the configuration files, documentation, and XML files to this folder.
  - **<SiteScope>\packages\workspace\package\_<>\template.** (Optional) The folder should contain the template files exported from SiteScope (performed in "Custom WMI Monitor" on page 145). Each template can contain various types of monitors, custom and regular.
- b. Copy extension files - optional

If the monitor references script or alert extension files in the SiteScope file system, copy them to the relevant folders in **<SiteScope root directory>\packages\workspace\extensions**:

- **\scripts.** Used for storing script files that are used to run shell commands or other scripts on the machine where SiteScope is running.
- **\scripts.remote.** Used for storing script files that are used for running a script that is stored on a remote machine.
- **\templates.mail.** Used for storing the file containing the format and content of alert messages sent by email.
- **\templates.mail.subject.** Used for storing the file containing the subject line of alert messages sent by email.
- **\templates.mib.** Used for storing the MIB files that are used to create a browsable tree that contains names and descriptions of the objects found during a traversal.
- **\templates.os.** Used for storing the shell commands to be run when monitoring remote UNIX servers.

**Note:**

- On exporting the files to a content package, the unique package ID is added to the script and template files as a suffix (before the file extension) under the relevant folder in the SiteScope root directory.
- As part of the import process, the **template.os** and **templates.mib** files are edited and the unique package ID is added to some properties inside the files.

- c. Export the content package to a zip file

Select the **Templates** context. In the template tree, right-click the template or template container that you want to export to a content package, and select **Export > Content Package**.

In the Export Content Package Wizard, enter details of the content package (manifest), and select the templates and files associated with these templates to include. For Wizard details, see Export Content Package Wizard.

For task details, see How to Create, Export, and Import a Custom Monitor Content Package and How to Create, Export, and Import a Template Extension Content Package in the Using SiteScope Guide.

**Note:** The Select Files page of the Wizard displays files from the **<SiteScope root directory>\packages\workspace\package\_<Package ID>** and **<SiteScope root directory>\packages\workspace\extensions** folders listed above, except for the **\META-INF** and **\templates** folders which are not displayed.

### 13. Share the custom monitor with other SiteScope users - optional

You can distribute a content package zip file by:

- Sending it to individual SiteScope users.
- Sharing it with other SiteScope users by uploading it to the Community Content for SiteScope page on [HPE Live Network](https://hpln.hpe.com/group/sitescope) (<https://hpln.hpe.com/group/sitescope>). HPE Live Network is an online community providing a central location for HP customers to share information and learn about add-on content, extensions and related activities across the HPE Software portfolio.

For task details, see How to Publish Content to the HPE Live Network Community.

## How to Debug a Custom Monitor Offline

This task describes the steps involved in offline debugging of a custom monitor script using a remote debugging environment. This makes the script development process easier, since it enables you to complete the code and see the debugged data inside the script during the data processing stage.

#### 1. Prerequisites

To perform offline debugging, the Eclipse IDE with Web Tools must be installed on a local machine.

#### 2. In SiteScope, enable the global custom monitor debugging setting in SiteScope Preferences

Select **Preferences > Infrastructure Preferences > Custom Monitor Settings**, and select the **Enable custom monitor debugging** check box.

#### 3. In SiteScope, create a custom monitor with offline debugging enabled

Create a custom monitor. For details, see the previous task.

When configuring the monitor settings, expand **Custom Monitor Settings**, and under the Data Processing Script section, select **Enable monitor debugging**.

Save the monitor.

#### 4. Copy the Custom Monitor Debugging Eclipse project to the debugging environment

The Custom Monitor Debugging Eclipse project is available (in zip format) from:

- **<SiteScope root directory>\examples\monitors\custom\CustomMonitorDebuggingEclipseProject**.



- The Community Content for SiteScope page on the HPE Live Network (<https://hpln.hp.com/group/community-content-sitescope>).

**Note:** Make sure you use the correct version of the Custom Monitor Debugging Eclipse project. SiteScope 11.23 is compatible with version 2.0 of the project (**SISProxy-2.0.min.js**).

5. Import the Custom Monitor Debugging project into Eclipse IDE
  - a. On the debugging environment, open Eclipse IDE and click **Import**.
  - b. Select **General > Existing Project into Workspace**, and click **Next**.
  - c. Select the Custom Monitor Debugging Eclipse project (zip file).
6. Copy the SiteScope Custom Monitor Data Processing Script to the Custom Monitor Debugging project
  - a. Copy the content of Data Processing Script from the SiteScope custom monitor to **MonitorScript.js** script.
  - b. Connect to the SiteScope monitor by entering the following in the **DebugConfiguration.js** file:
    - **host**. Name of the SiteScope server.
    - **port**. Port used by the SiteScope server.
    - **username**. Username for accessing the SiteScope server.
    - **password**. Password to access the SiteScope server.
    - **monitorPath**. Full path to the custom monitor to debug in SiteScope including the monitor name, separated by "/". For example, Group1/Group2/Group3/Custom Monitor Name.
7. Enable the debugger to use external jar files - optional (where the script uses external jar files)

If the monitor script uses external jar files, copy the jar files from **<SiteScope root directory>\packages\workspace\package\_<Package ID>\lib** to the **<JRE installation path>\lib\ext** directory on the debugging environment.
8. Run the debugger
  - a. In the Eclipse IDE, select **Debug Configuration**.
  - b. Select **Rhino JavaScript > Custom Monitor Debugging - MonitorScript.js**.
  - c. The debugger connects to SiteScope, and runs the script within the monitor.

SiteScope returns the data to the debugger and then disconnects. This enables the debugger to simulate the script running the same data.
9. Debug the script

Use Eclipse IDE to debug the script.

## How to Access the Monitor Configuration Parameters Exposed in the Script

### Data Script:

- You can access the configuration parameters for custom monitors in the data script using:

```
myContext.getInputData().getConfigurationParameter("<configuration parameter name>");
```

Example:

```
var monitorName = myContext.getInputData().getConfigurationParameter("monitorName");
```

The following monitor properties are exposed to the script (for all custom monitors):

- `monitorName`. The name of the monitor.
- `monitorDescription`. A description of the monitor.

The following monitor properties are exposed to the script for the Custom WMI monitor only:

- `server`. The name of the server from which you want to collect the data.
- You can set the summary string which is used as the monitor status in the SiteScope Dashboard using:  

```
myContext.getScriptResult().setSummary(<user's text summary>);
```

The default value is: `summary = <a set of metrics and their values>`
- You can set monitor availability which is displayed in the SiteScope Dashboard using:  

```
myContext.getScriptResult().setAvailability(<true/false>)
```

The default value is: `availability = true`

### Topology Script:

You can access the configuration parameters for custom monitors in the topology script using:

```
Framework.getDestinationAttributeAsObject("configuration").get("<configuration parameter name>")
```

To access data saved in the monitor storage (this is a place where you can save script data for use in future executions):

```
Framework.getDestinationAttributeAsObject("monitorStorage").get("<configuration parameter name>")
```

To access the list of metric names used in the script:

```
Framework.getDestinationAttributeAsObject("metrics")
```

## How to Import and Use a Custom WMI Monitor

After developing a custom monitor and creating a content package zip file, the content package can then be sent to specific users, or be published to the [HPE Live Network](https://hpln.hpe.com/group/sitescope) (<https://hpln.hpe.com/group/sitescope>) community enabling other users to import the monitor for their own use.

For details on using the Wizard, see Export Content Package Wizard.

### 1. Prerequisites

Only a SiteScope administrator user, or a user granted the **Add, edit or delete templates** permissions can import monitor templates from a content package. For details, see Permissions.

### 2. Access the custom monitor content package zip file

- If a content package zip file was sent to you, skip to the next step.
- If a content package was made available to the Community Content for SiteScope page on [HPE Live Network](https://hpln.hpe.com/group/sitescope), download the content package to your SiteScope machine. HPE Live Network is an online community providing a central location for HPE customers to share information and learn about add-on content, extensions and related activities across the HPE Software portfolio.

For task details, see How to download a template or content package from the HPE Live Network in the Using SiteScope Guide.

### 3. Import the custom monitor content package

- a. In SiteScope, select the **Templates** context. In the template tree, right-click the template container

into which you want to import the content package, and click **Import**.

- b. In the Content Import dialog box, select **Content package**, and click the **Browse** button. Navigate to the folder containing the package you want to import (packages are distributed in zip format). Click **Open**, and then click **OK**. For details on the Content Import dialog box, see Content Import Dialog Box in the Using SiteScope Guide.

For task details, see How to Create, Export, and Import a Custom Monitor Content Package and How to Create, Export, and Import a Template Extension Content Package in the Using SiteScope Guide.

#### 4. **Verify the template was imported successfully by checking it was added to the template tree**

The content package is copied to the **<SiteScope root directory>\packages\imported** folder, and a new folder is created with the name: **<Package/Zip Name>.zip\_<Package ID>**.

The folder contains:

- **\META-INF**. Contains the manifest file where information about the content package is stored.
- **\templates**. Contains files from which templates in this content package were imported into SiteScope.
- **<Package/Zip Name>**. Uncompressed package that contains the above-mentioned folders, the **\extensions** folder which contains script and alert template files referenced by monitors in the imported templates, and the folders used for Custom monitors:
  - **\classes**. Used for storing compiled Java classes.
  - **\conf** Used for storing configuration files, documentation, and XML files.
  - **\lib** Used for storing external jar files used by the monitor script. Note that the **\lib** folder is shared between all monitors imported in the same template.
- **<Package/Zip Name>.zip.properties**. This is the descriptor (manifest) file for content packages created in SiteScope 11.20, that is used in case of rollback, uninstall, or upgrade. The file contains the ID of the SiteScope template that was deployed, the location of the files in SiteScope, and other information about the content package.

The imported templates and dependency files can be used directly or modified as required.

Where script or alert templates are referenced in the user interface, the unique package ID is added as a suffix.

**Example:** ShortMail alert action template referenced in the Template field.

Action Type Settings	
Action name:	EMail
* Recipients:	Default
Addresses:	
* Subject:	Typical
* Template:	ShortMail_06b62f60-807c-4102-adea-9a7ebdd80e8b

## 5. Deploy the custom monitor template

After importing the custom monitor template, you can deploy the template to a group.

- a. In the template tree, right-click the custom monitor template you want to deploy, and select **Deploy Template**.
- b. 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 user interface details, see Select Group Dialog Box in the Using SiteScope Guide.
- c. In the Deployment Values dialog box, enter the required variable values in the entry boxes displayed, and click **OK**. The entry boxes displayed correspond to the template variables used in the template objects. For user interface details, see Deployment Values Dialog Box in the Using SiteScope Guide.

**Note:** When deploying the template or publishing changes in the template to deployed groups, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, because the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.

- d. Verify that the template was deployed successfully (the template objects should be added to the specified group in the monitor tree).

For task details, see How to Deploy Templates Using the User Interface in the Using SiteScope Guide.

## 6. Configure monitor status thresholds

When deploying the template, only the default metrics included with the monitor are displayed (custom metrics defined in the script do not exist until after the monitor has run).





After the monitor run, you can define thresholds for metrics that were resolved in the run. In the **Threshold Settings** panel of the custom monitor, select metrics for which you want to define thresholds in the **Condition** column by using variables or free text, or selecting default metrics from the drop-down list, and enter the value applicable to the metric parameter.


# UI Descriptions

## Custom WMI Monitor Settings

User interface elements are described below:

UI Element	Description
Main Settings	

UI Element	Description
<b>Server</b>	<p>Name of the server that you want to monitor. Select a server from the server list (only those Windows remote servers that have been configured in SiteScope with a WMI connection are displayed). Alternatively, click the <b>Add Remote Server</b> button to add a new server.</p> <p><b>Note:</b> When working in template mode, 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>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see "New/Edit Microsoft Windows Remote Server Dialog Box" in the Using SiteScope Guide.</p> <p><b>Note:</b> In the Add Microsoft Windows Remote Server dialog box, the <b>Method</b> field is automatically set to <b>WMI</b> (and cannot be changed), since this monitor can only use a Windows remote server configured with a WMI connection.</p>
<b>Script Parameters Table</b>	
	<b>Add Parameter.</b> Adds a new line to the Script Parameters table, enabling you to define parameters for use in the custom monitor script.
	<b>Delete Parameter.</b> Deletes the selected parameter.
<b>Parameter Name</b>	The name assigned to the parameter. All parameter names must be different.
<b>Parameter Value</b>	<p>The parameter value.</p> <p>If you want to hide a parameter value such as a password, select the <b>Hide Value</b> check box. The value is masked behind asterisks (*****) in the user interface.</p>
<b>Hide Value</b>	<p>Select to hide the parameter value in the Script Parameters table and in the custom monitor script. The value is masked behind asterisks (*****).</p> <p>This option is useful for an administrator in SiteScope when creating custom monitor templates, since it enables the monitor to be deployed without the parameter value being displayed in the monitor view.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> The hide option is editable when working in template mode only.</p>
<b>Configuration File</b>	Use the <b>Browse</b> button to select the configuration file. The configuration file must be a valid XML file. If it is not, then an error message is displayed. The XML configuration file is copied into the <code>conf</code> folder of the monitor.
<b>WMI Queries Table</b>	
	<b>New query.</b> Adds a new line to the WMI queries table, enabling you to enter a new query.
	<b>Edit query.</b> Opens the Query Editor, in which the selected WMI query is displayed and can be edited.

UI Element	Description
	<b>Delete query.</b> Enables you to delete the selected query.
<b>No</b>	<p>The query number. By default, you can add up to 10 queries to the table. The queries are run in the order in which they appear in the table.</p> <p><b>Note:</b> You can modify the number of queries that can be added to the table by changing the <b>Maximum number of queries</b> value in <b>Preferences &gt; Infrastructure Preferences &gt; Custom Monitor Settings</b>.</p>
<b>Queries</b>	Enter the WMI query you want to use. You can create or edit a query in the table (in line mode), or in the Query Editor. To open the Query Editor, click the <b>Edit query</b> button. It is recommended to use the Query Editor when adding or viewing long queries.
<b>Namespace</b>	<p>Enter the WMI namespace on which you want to perform the WQL query. Each namespace holds classes that expose different types of information.</p> <p><b>Example:</b> root\cimv2</p>
<b>Data Processing Script</b>	
<b>&lt;Script&gt;</b>	<p>The input data for the data processing script is displayed in this box.</p> <p>Define the script that parses the results and creates new metrics. For details on the monitor configuration properties in the script, including how to access them, and the monitor storage and metrics names, see <a href="#">"How to Access the Monitor Configuration Parameters Exposed in the Script" on page 153</a>.</p> <p><b>Note:</b> By default, the number of metrics that are allowed in custom monitors is 1000. You can modify this number by changing the <b>Maximum number of counters</b> value in <b>Preferences &gt; Infrastructure Preferences &gt; Custom Monitor Settings</b>.</p>

UI Element	Description
<b>Package path</b>	<p>Path generated by SiteScope where the files used for developing the monitor can be saved. This enables you to add the jars on which the monitor depends (if applicable), classes, configuration, and templates files to the monitor. The path is displayed as read only.</p> <p>Click the <b>Create Path</b> button to create a folder with a relative path in the SiteScope root directory (packages\workspace\package_&lt;unique ID&gt;). The path is displayed as read only.</p> <p>The folder contains the following subfolders into which you copy the files used to create the monitor:</p> <ul style="list-style-type: none"> <li>• <b>lib.</b> (Optional) Used for storing external jar files used by the monitor script. Note that you can use this monitor without external jars.</li> <li>• <b>classes.</b> (Optional) Used for storing Java compiled classes; note that they should be copied with the entire package folder structure.</li> <li>• <b>conf.</b> (Optional) Used for storing configuration files, documentation, and XML files.</li> <li>• <b>template.</b> (Mandatory) Used for storing the template files that contain the custom monitor. It must contain at least one template. Each template can contain various types of monitors; custom and regular.</li> </ul> <p><b>Note:</b> This field is displayed when working in monitor mode only. When working in template mode and the monitor is deployed, the content pack is imported into the path.</p> <p><b>Enable monitor debugging:</b> Select the checkbox to enable sending debugging logs for custom monitors to a remote debugging server. Note that custom monitor debugging must also be enabled in <b>Infrastructure Preferences</b>. (<b>Infrastructure Preferences</b> &gt; <b>Custom Monitor Settings</b> &gt; <b>Enable custom monitor debugging</b>).</p>
<b>Checksum</b>	Click <b>Calculate Checksum</b> to calculate the MD5 checksum of a specific folder and the script.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and limitations for the Custom WMI monitor.

- ["General Tips/Limitations" below](#)
- ["Monitor Specific Tips/Limitations" on the next page](#)
- ["Custom Monitor Logs" on the next page](#)

### General Tips/Limitations

- If a user-defined or imported Java package has the same name as an existing SiteScope or standard Java package, SiteScope ignores the user-defined/imported Java package.
- When setting custom monitor metrics with a string (non-numeric) value, the maximum and average values

in the Measurement Summary table of the Management Report are shown as 'n/a'. This also occurs if you change the metric value type, for example, if you set the metric with a numeric value, and later change it to a string value or vice versa.

- When deploying a custom monitor using a template, clearing the **Verify monitor properties with remote server** check box in the Deployment Values dialog box has no effect, because the monitor configuration properties in the template must be checked against the remote server on which the template is being deployed.
- When publishing changes to a template that contains a custom monitor, we recommend using the **Disable custom monitors while publishing changes** option (selected by default) in **Preferences > Infrastructure Preferences > Custom Monitor Settings**. The monitor is temporarily disabled before changes are published and is restored to the enabled state after changes have been made.
- Setting status thresholds using a baseline is not supported on user-defined metrics.
- You can use third-party .jar files without removing the JVM security from the registry by adding the `_scriptSandboxRuntimePermissions` property to the `<SiteScope root directory>\groups\master.config` file, and specifying the permitted jar files. For example, to use signed libraries `jopcagtbases.jar` and `jopcagtmessages.jar`, configure the parameter as follows: `_scriptSandboxRuntimePermissions=loadLibrary.jopcagtbases, loadLibrary.jopcagtmessages`.  
For the types of runtime permissions that can be used, see Runtime Permission class in the [Java API documentation](http://docs.oracle.com/javase/7/docs/api/java/lang/RuntimePermission.html) (<http://docs.oracle.com/javase/7/docs/api/java/lang/RuntimePermission.html>).

## Monitor Specific Tips/Limitations

- SiteScope does not support WMI event handling or WMI method execution.
- It is not recommended to have more than 4000 monitors using WMI.
- Support for 32-bit access to the VSS WMI provider on a 64-bit operating system was removed in Windows Server 2008. Therefore, any 32-bit program that attempts to enumerate Win32\_ShadowCopy instances (or instances of any VSS class) will fail on 64-bit Windows Server 2008.
- When a metric or object is shared between resources, SiteScope is unable to receive data for the metrics and the query fails. If other metrics are referenced in the same query, they also fail to receive data. For details and troubleshooting information, refer to <http://support.microsoft.com/kb/836802>.
- If running a dynamic query from within a data processing script fails, an exception is thrown.
- Due to a WMI Interface problem on Microsoft Windows Server 2003, the Custom WMI monitor is unable to get the correct values for **CurrentClockSpeed** and **MaxClockSpeed** from WMI namespace when SiteScope is running on a Windows Server 2003 platform.

## Custom Monitor Logs

- Errors in the monitor (including errors in the script) are written to the SiteScope logs in the same way as for any other monitor. Check the **error.log** and **RunMonitor.log** files.
- Error messages from the script are displayed in the **custom\_monitor.log** file located in `<SiteScope root directory>\logs\custom_monitors`. This log can be used for info, warning, error, and debug messages from running the script.

To change the log level to **DEBUG** mode, in `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties`, change `$(loglevel)` to **DEBUG** in the following paragraph:

```
# Custom monitors category
log4j.category.CustomMonitor=$(loglevel),custom.monitor.appender
log4j.additivity.CustomMonitor=false change
```



# Chapter 21: Database Counter Monitor

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. The error and warning thresholds for the monitor can be set on one or more database server performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Database Counter monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["Setup Requirements and User Permissions" below](#)
- ["IPv6 Addressing Supported Protocols" on page 163](#)
- ["Database Counter Topology" on page 163](#)
- ["License Consumption" on page 164](#)

## Supported Platforms/Versions

This monitor supports monitoring on any database with a valid JDBC driver that supports SQL queries.

## Setup Requirements and User Permissions

The following are several key requirements for using the Database Counter 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. If the file is in zip format, unzip the contents to a temporary directory. 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.mercury.jdbc.sqlserver.SQLServerDriver**. DataDirect driver from DataDirect Technologies. It is a driver for those Microsoft SQL databases that use Windows authentication. For details on installing the driver, see the note below.

**Note:** To install the MSSQL JDBC driver:

- 1). Download the MSSQL JDBC driver from the [Microsoft Download Center](#)

(<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2505>), and unzip the contents to a temporary directory.

2). Copy the **sqljdbc4.jar** file to the **<SiteScope root directory>\WEB-INF\lib\** subdirectory.

3). Restart the SiteScope service.

4). Use the Database Connection Tool for connection tuning:

**Database Connection URL:** jdbc:sqlserver://<IP

Address>:<port>;InstanceName=<name>;DatabaseName=<name>

**Database Driver:** com.microsoft.sqlserver.jdbc.SQLServerDriver

5). Create the desired database monitor type.

- **com.mercury.jdbc.oracle.OracleDriver.** A driver for Oracle databases. When using the driver deployed with SiteScope, the database connection URL has the form of: jdbc:mercury:oracle://<server name or IP address>:<database server port>;sid=<sid>

**Note:** The URL format may differ if you are using another JDBC driver, since the JDBC URL depends on the driver.

- **oracle.jdbc.driver.OracleDriver.** SiteScope supports the following categories of JDBC driver supplied by Oracle that are compatible with Java 7:
  - JDBC thin driver for Oracle databases.
  - JDBC OCI (thick) driver. For details on accessing Oracle databases using OCI driver, see ["How to access Oracle databases using OCI driver" on page 165](#).
- **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:mercury:sqlserver://<hostname or FQDN>:1433;DatabaseName=master;AuthenticationMethod=type2**  
where <hostname or FQDN> is the name of the host where the database is running.
- **jdbc:oracle:thin:@<hostname or FQDN>:<port>/<service>**  
where <hostname or FQDN> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <service> is the Oracle service name.  
When monitoring Oracle RAC databases, the database connection URL has the form of:  
jdbc:oracle:thin:@SCAN (Single Client Access Name) listener>:<port>/<database service name>
- **jdbc:postgresql://<hostname or FQDN>:<port>/<dbname>**  
where <hostname or FQDN> 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, only one instance of each type of JDBC driver client should be 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 `ojdbc6.jar` files from two different versions of Oracle is unlikely to work.

- Database drivers that have timeout problems (where database queries processed with these drivers exceed the timeout specified in the monitor's **Query timeout** field) can be specified in the **Timeout proxied query drivers list** field (in **Preferences > Infrastructure Preferences > General Settings**). These drivers are queried separately with a monitor-based timeout.
- 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.

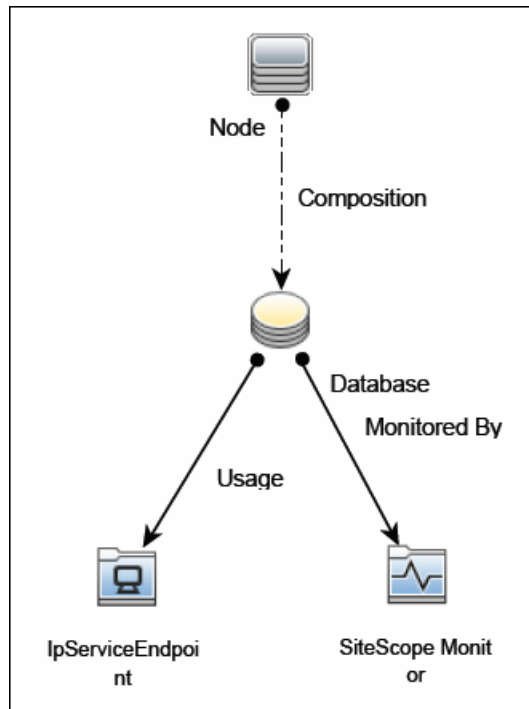
## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the TCP (JDBC) protocol. Support for IPv6 might also depend on the JDBC driver being used.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## Database Counter Topology

The Database Counter monitor can identify the topology of the database system being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see [Reporting Discovered Topologies to BSM](#) in the [Using SiteScope Guide](#).

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host.

## Tasks

This section includes:

- ["How to Configure the Database Counter Monitor" below](#)
- ["How to access Oracle databases using OCI driver" on the next page](#)

### How to Configure the Database Counter Monitor

#### 1. Prerequisites

Before configuring the monitor, make sure you have the necessary ["Setup Requirements and User Permissions" on page 161](#).

#### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the [UI Descriptions](#) section below.

**Tip:** The **Database Connection Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Database Connection Tool in the Using SiteScope Guide.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HPE Integration Settings** (the default setting). For details on the monitor topology, see "[Database Counter Topology](#)" on page 163.

For user interface details, see "[BSM Integration Data and Topology Settings](#)" in the Using SiteScope Guide.

## How to access Oracle databases using OCI driver

You can monitor an Oracle database using an OCI driver. If the port or SID are changed, you only need to make the change in the **tnsnames.ora** file (the SiteScope Oracle monitors remain unchanged).

1. On the SiteScope server, install the version of Oracle client that you are using.
2. Connect to the Oracle database using the Oracle OCI driver.
  - Set **ORACLE\_HOME** environment variable (**ORACLE\_HOME** is the folder where the Oracle client or database has been installed).
  - Add **ORACLE\_HOME\lib** to System PATH (on Windows platforms), or **LD\_LIBRARY\_PATH** env variable (on UNIX platforms).
  - Set **CLASSPATH** environment variable to use Oracle JDBC driver from **ORACLE\_HOME\jdbc\lib**.
3. In the **\oracle\oraX\network\admin\tnsnames.ora** file, configure the service name. You can test this using a SQL+ tool or the SiteScope Database Connection tool (see Database Connection Tool in the Using SiteScope Guide).
4. Add a database monitor within SiteScope, and configure the following settings in the Monitor Settings panel:
  - **Database connection URL:** `jdbc:oracle:oci8:@<service name>`
  - **Database driver:** `oracle.jdbc.driver.OracleDriver`
  - Enter the database user credentials in the **Database user name** and **Database password** boxes.
5. Copy the `ocijdbc11.dll` into **ORACLE\_HOME\java\lib** and `ojdbc5.jar` into **ORACLE\_HOME\Java\lib\ext** or **ORACLE\_HOME\Web-INF\lib**. You must manually copy these if the OS environment PATH does not load them.

## UI Descriptions

### Database Counter Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Database connection URL</b>	<p>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>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>Driver used to connect to the database.</p> <p><b>Example:</b> <code>org.postgresql.Driver</code></p> <p><b>Tip:</b> You can specify database drivers that have timeout problems (where database queries processed with these drivers exceed the timeout specified in the monitor's <b>Query timeout</b> field) in the <b>Timeout proxied query drivers list</b> field (in <b>Preferences &gt; Infrastructure Preferences &gt; General Settings</b>). These drivers are queried separately with a monitor-based timeout.</p>
<b>Database machine name</b>	<p>Identifier for the target database server, as it should be reported to BSM.</p> <p><b>Note:</b> This field is used only for topology reporting.</p>
<b>Database port</b>	<p>Port number, for the target database server, as it should be reported to BSM. You can specify the port manually. If none is specified, the monitor attempts to detect the port from the database connection URL. If it fails, topology is still reported, just without <code>IpServiceEndpoint</code>.</p> <p><b>Note:</b> This field is used only for topology reporting.</p>

UI Element	Description
<b>Database instance name</b>	<p>Name of the database instance, as it should be reported to BSM.</p> <p>For SQL servers, the monitor automatically detects and populates this field from the database connection URL.</p> <p>For Oracle, the monitor automatically detects the instance name from the database connection URL without populating the field.</p> <p>If the field is empty and auto detection fails, no topology is reported and the default CI type <b>Note</b> is displayed in the HP Integration Settings panel.</p> <p><b>Note:</b> This field is used only for topology reporting.</p>
<b>Divisor query</b>	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.
<b>No cumulative counters</b>	Turns 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>Credentials</b>	<p>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 How to Configure Credential Preferences in the Using SiteScope Guide.</li> </ul>
<b>No divide counters</b>	<p>Turns 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>Counters</b>	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>Opens the Select Counters Form, enabling you to 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>

UI Element	Description
<b>Database Connection Settings</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 JDBC, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>	
<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>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>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>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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Tips/Limitations

- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- 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. For details, see JDBC Global Options in the Using SiteScope Guide.



# Chapter 22: Database Query Monitor

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Database Query monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["What to Monitor" below](#)
- ["Setup Requirements and User Permissions" below](#)
- ["IPv6 Addressing Supported Protocols" on page 171](#)
- ["Database Query Topology" on page 171](#)
- ["License Consumption" on page 172](#)

## Supported Platforms/Versions

This monitor supports monitoring on any database with a valid JDBC driver that supports SQL queries.

## 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. If the file is in zip format, unzip the contents to a temporary directory. 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.mercury.jdbc.sqlserver.SQLServerDriver.** DataDirect driver from DataDirect Technologies. It is a driver for those Microsoft SQL databases that use Windows authentication. For details on installing the driver, see the note below.

**Note:** To install the MSSQL JDBC driver:

- 1). Download the MSSQL JDBC driver from the [Microsoft Download Center](http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=11774) (<http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=11774>), and unzip the contents to a temporary directory.
- 2). Copy the **sqljdbc4.jar** file to the **<SiteScope root directory>\WEB-INF\lib\** subdirectory.
- 3). Restart the SiteScope service.

- 4). Use the Database Connection Tool for connection tuning:

**Database Connection URL:** jdbc:sqlserver://<IP

Address>:<port>;InstanceName=<name>;DatabaseName=<name>

**Database Driver:** com.microsoft.sqlserver.jdbc.SQLServerDriver

- 5). Create the desired database monitor type.

- **com.mercury.jdbc.oracle.OracleDriver.** A driver for Oracle databases. When using the driver deployed with SiteScope, the database connection URL has the form of: jdbc:mercury:oracle://<server name or IP address>:<database server port>;sid=<sid>

**Note:** The URL format may differ if you are using another JDBC driver, since the JDBC URL depends on the driver.

- **oracle.jdbc.driver.OracleDriver.** SiteScope supports the following categories of JDBC driver supplied by Oracle that are compatible with Java 7:
  - JDBC thin driver for Oracle databases.
  - JDBC OCI (thick) driver. For details on accessing Oracle databases using OCI driver, see ["How to Access Oracle Databases Using OCI Driver" on page 173](#).
- **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:mercury:sqlserver://<hostname or FQDN>:1433;DatabaseName=master;AuthenticationMethod=type2**  
where <hostname or FQDN> is the name of the host where the database is running.

- **jdbc:oracle:thin:@<hostname or FQDN>:<port>/<service>**

where <hostname or FQDN> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <service> is the Oracle service name.

- 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.
- Database drivers that have timeout problems (where database queries processed with these drivers exceed the timeout specified in the monitor's **Query timeout** field) can be specified in the **Timeout proxied query drivers list** field (in **Preferences > Infrastructure Preferences > General Settings**). These drivers are queried separately with a monitor-based timeout.
- 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.

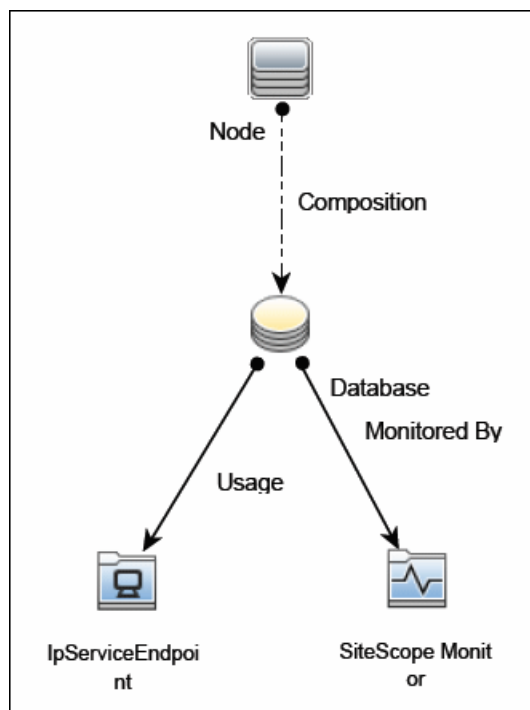
## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports IPv6 addresses in the TCP (JDBC) protocol. Support for IPv6 might also depend on the JDBC driver being used.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## Database Query Topology

The Database Query monitor can identify the topology of the database system being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see [Reporting Discovered Topologies to BSM](#) in the [Using SiteScope Guide](#).

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitored host.

## Tasks

This section includes:

- ["How to Configure the Database Query Monitoring Environment"](#) below
- ["How to Access Oracle Databases Using OCI Driver"](#) on the next page
- ["How to Access Oracle Databases Without Using ODBC"](#) on page 174
- ["How to Enable SiteScope to Monitor an Informix Database"](#) on page 175
- ["How to Enable SiteScope to Monitor a MySQL Database"](#) on page 175
- ["How to Enable SiteScope to Monitor a Sybase Database"](#) on page 176

### How to Configure the Database Query Monitoring Environment

#### 1. Prerequisites

There are several key requirements for using this monitor. For details, see ["Setup Requirements and User Permissions"](#) on page 169.

2. Configure the database driver
  - You can monitor an Oracle database using an OCI driver. For details, see ["How to Access Oracle Databases Using OCI Driver" below](#).
  - You can monitor an Oracle database using the Oracle Thin JDBC Driver. For details, see ["How to Access Oracle Databases Without Using ODBC" on the next page](#).
3. Enable SiteScope to monitor the database
  - For details on enabling SiteScope to monitor an Informix database, see ["How to Enable SiteScope to Monitor an Informix Database" on page 175](#).
  - For details on enabling SiteScope to monitor a MySQL database, see ["How to Enable SiteScope to Monitor a MySQL Database" on page 175](#).
  - For details on enabling SiteScope to monitor a Sybase database, see ["How to Enable SiteScope to Monitor a Sybase Database" on page 176](#).
4. Troubleshoot driver or database errors

To troubleshoot possible errors using the Oracle Thin Driver, MySQL Driver, or Sybase database, see ["Tips/Troubleshooting" on page 180](#).
5. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:**

- The **Database Connection Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Database Connection Tool in the Using SiteScope Guide.
- 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.
- You can also modify the default number of columns, rows, and characters that are displayed for the Database Query monitor in the SiteScope Dashboard by changing the **DB maximum columns**, **DB maximum rows**, and **DB maximum value length** settings in **Preferences > Infrastructure Preferences > Monitor Settings**.
- When setting the **round trip time** counter in Threshold Settings, counter values are in milliseconds, whereas in the Dashboard summary they are displayed in seconds.

## How to Access Oracle Databases Using OCI Driver

You can monitor an Oracle database using an OCI driver. If the port or SID are changed, you only need to make the change in the **tnsnames.ora** file (the SiteScope Oracle monitors remain unchanged).

1. On the SiteScope server, install the version of Oracle client that you are using.
2. Connect to the Oracle database using the Oracle OCI driver.

- Set **ORACLE\_HOME** environment variable (**ORACLE\_HOME** is the folder where the Oracle client or database has been installed).
  - Add **ORACLE\_HOME\lib** to System PATH (on Windows platforms), or **LD\_LIBRARY\_PATH** env variable (on UNIX platforms).
  - Set **CLASSPATH** environment variable to use Oracle JDBC driver from **ORACLE\_HOME\jdbc\lib**.
3. In the `\oracle\oraX\network\admin\tnsnames.ora` file, configure the service name. You can test this using a SQL+ tool or the SiteScope Database Connection tool (see Database Connection Tool in the Using SiteScope Guide).
  4. Add a database monitor within SiteScope, and configure the following settings in the Monitor Settings panel:
    - **Database connection URL:** `jdbc:oracle:oci8:@<service name>`
    - **Database driver:** `oracle.jdbc.driver.OracleDriver`
    - Enter the database user credentials in the **Database user name** and **Database password** boxes
  5. Copy the `ocijdbc11.dll` into `ORACLE_HOME\java\lib` and `ojdbc5.jar` into `ORACLE_HOME\Java\lib\ext` or `ORACLE_HOME\Web-INF\lib`. You must manually copy these if the OS environment PATH does not load them.

## How to Access Oracle Databases Without Using ODBC

If you want to monitor an Oracle database without using ODBC, you can use the Oracle Thin JDBC Drivers.

1. 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).
2. Copy the downloaded driver package into the **<SiteScope root directory>\WEB-INF\lib** subdirectory.

**Note:** Do not extract the files from the archive file.

3. Stop and restart the SiteScope service.
4. 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`

When monitoring Oracle RAC databases, the database connection URL has the form of:

`jdbc:oracle:thin:@SCAN (Single Client Access Name) listener:<port>/<database service name>`

**Note:** After the word `thin` is a colon (:) and an at (@) symbol.

- **Database driver.** Enter the following string: `oracle.jdbc.driver.OracleDriver`.

## How to Enable SiteScope to Monitor an Informix Database

Monitoring an Informix database requires the use of a JDBC driver.

1. Download the Informix JDBC driver from Informix. See the Informix Web site for details.
2. Uncompress the distribution file.
3. Open a DOS window and go to the **jdbc140jc2** directory.
4. Unpack the driver by running the following command:

```
c:\SiteScope\java\bin\java -cp . setup
```

5. Copy **ifxjdbc.jar** to the **<SiteScope root directory>\WEB-INF\lib** subdirectory.
6. Stop and restart SiteScope.
7. 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`

## How to Enable SiteScope to Monitor a MySQL Database

Monitoring a MySQL database requires the use of a JDBC driver.

1. Download the MySQL JDBC driver from the MySQL web site (<http://www.mysql.com>).
2. Uncompress the distribution file.
3. Copy the .jar file into the **<SiteScope root directory>\WEB-INF\lib** directory.
4. Stop and restart SiteScope.
5. 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`

## How to Enable SiteScope to Monitor a Sybase Database

To use JDBC drivers with your Sybase SQL server, perform the following steps:

1. 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, look for a driver in the Jconnect directory.
2. Place the zip file in the **<SiteScope root directory>\WEB-INF\lib** directory. Do not extract the zip file.
3. Stop and restart the SiteScope service.
4. 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`



## UI Descriptions

### Database Query Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Database connection URL</b>	<p>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 test. 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 &lt;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>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 <b>&lt;SiteScope root directory&gt;\WEB-INF\lib\</b> directory.</p> <p><b>Default value:</b> <code>sun.jdbc.odbc.JdbcOdbcDriver</code></p> <p><b>Tip:</b> You can specify database drivers that have timeout problems (where database queries processed with these drivers exceed the timeout specified in the monitor's <b>Query timeout</b> field) in the <b>Timeout proxied query drivers list</b> field (in <b>Preferences &gt; Infrastructure Preferences &gt; General Settings</b>). These drivers are queried separately with a monitor-based timeout.</p>

UI Element	Description
<b>Database user name</b>	<p>User name used to log on to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystems JDBC-ODBC bridge driver, <code>sun.jdbc.odbc.JdbcOdbcDriver</code>), you can leave this blank and choose Windows Authentication when you setup the ODBC connection.</p> <p>With Windows 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>
<b>Database password</b>	<p>Password used to log on to the database.</p> <p>If you are using Microsoft SQL server and the default driver (Sun Microsystems JDBC ODBC bridge driver (<code>sun.jdbc.odbc.JdbcOdbcDriver</code>), you can leave this blank and choose Windows Authentication when you create the ODBC connection.</p> <p>With Windows Authentication, SiteScope connects using the login account of the SiteScope service.</p>
<b>Query</b>	<p>SQL query to test.</p> <p><b>Example:</b> <code>select * from sysobjects</code></p>
<b>Match content</b>	<p>Text string 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. The search is case sensitive.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>You can also perform a Perl regular expression match by enclosing the string in forward slashes, with an <code>i</code> after the trailing slash indicating case-insensitive matching. For example, <code>/href=Doc\d+\.html/</code> or <code>/href=doc\d+\.html/i</code>.</li> <li>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. For example, <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.</li> </ul> <p>For details on regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.</p>
<b>Open Tool</b>	<p>Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.</p>

UI Element	Description
<b>File path</b>	<p>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>
<b>Column labels</b>	<p>Field labels for all 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 the labels that are returned by the Query string entered above.</p>
<b>Database machine name</b>	<p>Text identifier describing the database server that this monitor is monitoring if you are reporting monitor data to an installation of BSM.</p> <p><b>Note:</b> This field is used only for topology reporting.</p>
<b>Database port</b>	<p>Port number, for the target database server, as it should be reported to BSM. You can specify the port manually. If none is specified, the monitor attempts to detect the port from the database connection URL. If it fails, topology is still reported, just without IpServiceEndpoint.</p> <p><b>Note:</b> This field is used only for topology reporting.</p>
<b>Database instance name</b>	<p>Name of the database instance, as it should be reported to BSM.</p> <p>For SQL servers, the monitor automatically detects and populates this field from the database connection URL.</p> <p>For Oracle, the monitor automatically detects the instance name from the database connection URL without populating the field.</p> <p>If the field is empty and auto detection fails, no topology is reported and the default CI type <b>Node</b> is displayed in the HP Integration Settings panel.</p> <p><b>Note:</b> This field is used only for topology reporting.</p>
<p><b>Database Connection Settings</b></p> <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 JDBC, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>	

UI Element	Description
Use connection pool	Enables SQL connection sharing. This means that you use a connection pool rather than open and close a new connection for each monitor query. <b>Default value:</b> Selected
Physically close if idle connection count exceeds	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. <b>Default value:</b> 10
Idle connection timeout	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
Query timeout	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

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and limitations for the Database Query monitor.

### General Tips

- If you require multiple columns in the monitor output, you can use the **\_databaseMaxColumns** property in the **<SiteScope root directory>\groups\master.config** file or the **DB maximum columns** setting in **Preferences > Infrastructure Preferences > Monitor Settings** to adjust the maximum number of columns displayed in the SiteScope Dashboard (the default is 10 columns). You can also change the maximum number of rows processed by DB monitors (**DB maximum rows**) and the maximum length, in characters, of the data processed by DB monitors (**DB maximum value length**). The default maximum number of rows is 1, and the default maximum value length is 200 characters.
- When using the Database Connection Tool to apply properties to the monitor, you must enter the credential data manually (if you select a credential profile the credential data is lost).
- You can set additional database options that affect all resources that connect to the database in the JDBC Global Options in **Preferences > General Preferences**. For details, see JDBC Global Options in the Using SiteScope Guide.
- When setting the **round trip time** counter in Threshold Settings, counter values are in milliseconds,

whereas in the Dashboard summary they are displayed in seconds.

### 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, 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 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 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 enabling SiteScope to monitor a MySQL database, you get an authorization error in the Database Query monitor, 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.
- **error, driver connect error, com/sybase/jdbc/SybDriver.** Verify 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** field is correct.

# Chapter 23: DB2 JDBC Monitor

Use this monitor to monitor availability and proper functioning of DB2 servers. 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. The error and warning thresholds for the monitor can be set on up to ten DB2 server performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the DB2 JDBC monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["DB2 JDBC Topology" below](#)
- ["License Consumption" on the next page](#)

### Supported Platforms/Versions

- This monitor supports monitoring DB2 8.x, 9.x, and 10.1 servers.
- It supports all operating systems with a supported JDBC driver and DB2 snapshot feature.

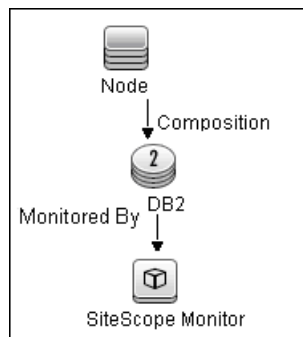
### IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the TCP (JDBC) protocol. Support for IPv6 might also depend on the JDBC driver being used.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

### DB2 JDBC Topology

The DB2 JDBC monitor can identify the topology of the DB2 system being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

# Tasks

## How to Configure the DB2 JDBC Monitor

### 1. Prerequisites

- 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>\WEB-INF\lib** folder.
- This monitor uses the Snapshot mirroring functionality supported by DB2. You must enable the Snapshot Mirror on your DB2 instance to retrieve counters. For details, refer to the relevant IBM DB2 documentation.

**Note:** Since DB2 JDBC monitors are based on JDBC connections, there is no binding with any specific operation systems.

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** The **Database Connection Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Database Connection Tool in the Using SiteScope Guide.

### 3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "[DB2 JDBC Topology](#)" on page 182.

For user interface details, see BSM Integration Data and Topology Settings in the Using SiteScope Guide.

## UI Descriptions

### DB2 JDBC Monitor Settings

User interface elements are described below:

UI Element	Description
<b>DB2 server</b>	Address or name of the server where the DB2 database is running.
<b>Port</b>	Port on which the DB2 database accepts connections. <b>Default value:</b> 50000
<b>Database</b>	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>	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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>Partition</b>	Partition to monitor. -1 is the current partition; -2 is all partitions. <b>Default value:</b> -1
<b>Calculate rate</b>	Calculates rates for counter values rather than the actual values returned from the monitored server. <b>Example:</b> If a counter counts logins and every second an average of two users log on to the database, the counter keeps growing. Selecting this option, the monitor displays the value 2, which means 2 user logins per second.



UI Element	Description
<b>Counters</b>	Server performance counters to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</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>Database Connection Settings</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 JDBC, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.</p>	
<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>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>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>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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

acc_curs_blk	int_rows_inserted rows_deleted	pool_index_from_estore
active_sorts	int_rows_updated	pool_index_l_reads
agents_created_empty_pool	local_cons	pool_index_p_reads
agents_from_pool	local_cons_in_exec	pool_index_to_estore
agents_registered	lock_escals	pool_index_writes
agents_stolen	lock_list_in_use	pool_lsn_gap_clns
agents_waiting_on_token	lock_timeouts	pool_read_time
appl_section_inserts	lock_wait_time	pool_write_time
appl_section_lookups	lock_waits	post_threshold_sorts
appls_cur_cons	lock_waits locks_held	prefetch_wait_time
appls_in_db2	locks_held	rej_curs_blk
binds_precompiles	locks_waiting	rem_cons_in
cat_cache_heap_full	log_reads	rem_cons_in_exec
cat_cache_inserts	log_writes	rollback_sql_stmts
cat_cache_lookups	num_assoc_agents	rows_deleted
cat_cache_overflows	num_gw_conn_switches	rows_inserted
comm_private_mem	open_loc_curs	rows_read
commit_sql_stmts	open_loc_curs_blk	rows_selected
con_local_databases	open_rem_curs	rows_updated
ddl_sql_stmts	open_rem_curs_blk	rows_written
deadlocks	pipelined_sorts_accepted	sec_logs_allocated
direct_read_reqs	pipelined_sorts_requested	select_sql_stmts
direct_read_time	pkg_cache_inserts	sort_heap_allocated
direct_reads	pkg_cache_lookups	sort_overflows
direct_write_reqs	pkg_cache_lookups direct_reads	static_sql_stmts
direct_write_time	pkg_cache_num_overflows	total_hash_joins
direct_writes	pool_async_data_read_reqs	total_hash_loops
dynamic_sql_stmts	pool_async_data_reads	total_log_used
failed_sql_stmts	pool_async_data_writes	total_sec_cons
files_closed	pool_async_index_reads	total_sort_time
hash_join_overflows	pool_async_index_writes	total_sorts
hash_join_small_overflows	pool_async_read_time	uid_sql_stmts
idle_agents	pool_async_write_time	uow_lock_wait_time
inactive_gw_agents	pool_data_from_estore	uow_log_space_used
int_auto_rebinds	pool_data_l_reads	x_lock_escals
int_commits	pool_data_p_reads	
int_deadlock_rollbacks	pool_data_to_estore	
int_rollbacks	pool_data_writes	
int_rows_deleted	pool_drty_pg_steal_clns sort_overflows	
int_rows_inserted	pool_drty_pg_thrsh_clns	

## Tips/Troubleshooting

### General Tips/Limitations

- SiteScope DB2 10.1 supports the same tables and counters that are available with DB2 8 and 9 only; it does not support the additional tables and counters that were added in DB2 10.1.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** option in the Deployment Values dialog box.

- 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. For details, see JDBC Global Options in the Using SiteScope Guide.
- When SiteScope is connected to BSM 9.2x or earlier, the previous name for this monitor (DB2 8.x and 9.x) is displayed in the Metrics and Indicators tab of System Availability Management Administration.

# Chapter 24: DHCP Monitor

This monitor enables you to monitor 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the DHCP monitor.

## Learn About

### DHCP Monitor Overview

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.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitored host

## Tasks

### How to Configure the DHCP Monitor

#### 1. Prerequisites

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.

- Download the JDHCP library (either in .zip or in .tar.gz format).
- Extract the file named **JDHCP.jar** and copy it to the **<SiteScope root directory>\WEB-INF\lib** directory.
- After installing the **JDHCP.jar** file, restart the SiteScope service.

#### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### DHCP Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Requested client address IPv4</b>	IPv4 address of the client to request from the DHCP server (optional).
<b>Timeout (seconds)</b>	Amount of time, in seconds, to wait for a response from a DHCP server. <b>Default value:</b> 10 seconds
<b>DHCP Server IPv4</b>	IPv4 address of the DHCP server for monitoring (optional). The DHCP server can be located on the same or a different subnet to the SiteScope server, according to the <b>MAC address</b> option selected below.
<b>MAC address</b>	MAC address of the network adapter on the SiteScope server. <ul style="list-style-type: none"><li>• <b>&lt;MAC addresses&gt;</b>. Lists the available MAC addresses. When a listed MAC address is selected, the DHCP monitor can monitor a DHCP server located on the same subnet, or on a different subnet to the SiteScope server.</li><li>• <b>Random address</b>. When selected, the DHCP monitor can only monitor a DHCP server that is located on the same subnet as the SiteScope server.</li></ul>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Chapter 25: Directory Monitor

The Directory monitor enables you to monitor an entire directory and report 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Directory monitor.

## Learn About

This section includes:

- ["Directory Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["License Consumption" on the next page](#)

### 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.

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.

### Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see ["How to Configure the HP NonStop Resources Monitor" on page 307](#).

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor  Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

## Tasks

### How to Configure the Directory Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Directory Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>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>

UI Element	Description
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Directory path</b>	<p>Directory that you want to monitor.</p> <ul style="list-style-type: none"> <li>• To monitor directories on a remote Windows 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 on 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 on 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 Configuring SiteScope to Monitor Remote Windows Servers in the Using SiteScope Guide.</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 in the Using SiteScope Guide.</p>
<b>No subdirectories</b>	Subdirectories are not included in the match count.
<b>File name match</b>	Text or an expression to match against. Only file names which match are counted in the totals.

**Note:** For information on configuring setting panels that are common to all monitors, see Common



Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- # of files
- Total disk space used
- first time since modified - This counter shows the modification date for the latest accessed file in the directory. If the directory contains no files, it shows the time that the last file was removed from the directory, or the time that the directory was created.

## Tips/Troubleshooting

### General Tips/Limitations

When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

# Chapter 26: Disk Space Monitor (Deprecated)

Use the Disk Space monitor to track how much disk space is currently in use on your server.

**Note:** The Disk Space monitor was deprecated and replaced by the ["Dynamic Disk Space Monitor" on page 201](#). Disk Space monitors configured in previous versions still work when upgrading to SiteScope 11.2x.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Disk Space monitor.

## Learn About

This section includes:

- ["Disk Space Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)

## 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 failed 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 in the Using SiteScope Guide.

**Note:** There is also a dynamic version of this monitor that automatically adds or removes counters and thresholds that measure the disk according to changes in the environment. For details, see ["Dynamic Disk Space Monitor" on page 201](#).

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms, and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see ["How to Configure the HP NonStop Resources Monitor" on page 307](#).
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.
- To monitor Microsoft Windows Server 2008 using WMI, install the Microsoft hot fix

(<http://support.microsoft.com/kb/961435>) on the target Windows system.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

# Tasks

## How to Configure the Disk Space Monitor

### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- 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>`).

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** The **Performance Counters Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Performance Counters Tool in the Using SiteScope Guide.

## UI Descriptions

### Disk Space Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>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></p> <ul style="list-style-type: none"><li>Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li><li>When working in template mode, 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></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Disk/File system</b>	<p>Disk drive to monitor.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### Tips

This monitor supports setting fractional thresholds which are more useful than setting whole number thresholds when monitoring large disks (such as 1 terabyte and larger).

### Troubleshooting and Limitations

#### WMI Returns Incorrect Disk Space Values

Due to a limitation with WMI, the WMI connection method returns incorrect results when this monitor is used on Windows Server 2008.

**Workaround:** To monitor Windows Server 2008 using WMI, install the Microsoft hot fix (<http://support.microsoft.com/kb/961435/en-us>) on the target Windows system.

# Chapter 27: DNS Monitor

This monitor enables you to monitor your Domain Name Servers (DNS) to verify that they are working properly.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the DNS monitor.

## Learn About

### DNS Monitor Overview

Use the DNS monitor to monitor your Domain Name Servers (DNS) 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).

The DNS monitor checks your DNS server by using the network; verifies that the DNS server is accepting requests; verifies that the address for a specific domain name can be found; and returns a status and writes it in the monitoring log file with each running.

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.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license for 10 monitors

## Tasks

### How to Configure the DNS Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** The **DNS Lookup Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or

editing a monitor, click the **Use Tool** button. For details on the tool, see DNS Tool in the Using SiteScope Guide.

## UI Descriptions

### DNS Monitor Settings

User interface elements are described below:

UI Element	Description
<b>IP address of DNS server to monitor</b>	IP address of the DNS server that you want to monitor. <b>Example:</b> 206.168.191.1
<b>Host name to resolve</b>	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>IP address or addresses mapped to the host to verify that it resolves correctly</b>	IP address or addresses that are mapped to the <b>Host name to resolve</b> (domain name) entered above. You can use the DNS monitor to verify that a host name or domain name resolves to the correct IP address or addresses.  <b>Note:</b> If you enter more than one IP address, the monitor reports a status of <i>good</i> , even if only one of the IP addresses that you enter is mapped correctly to the <b>Host name 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 name to resolve</b> . When entering multiple IP addresses, separate them with a comma (",").

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### Troubleshooting and Limitations

- 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 have 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.



# Chapter 28: Dynamic Disk Space Monitor

The Dynamic Disk Space monitor tracks how much disk space is currently in use on your server. When dynamic monitoring is configured, the counters and thresholds are automatically updated as disks are added to or removed from the server. This enables you to configure the monitor once, and leave it to detect disks and file systems changes.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Dynamic Disk Space monitor.

## Learn About

This section includes:

- ["Dynamic Disk Space Monitor Overview" below](#)
- ["Supported Platforms/Versions" on the next page](#)
- ["Monitor Run Frequency" on the next page](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)
- ["Dynamic Disk Space Monitor Topology" on the next page](#)
- ["License Consumption" on page 203](#)

## Dynamic Disk Space Monitor Overview

Use the Dynamic Disk Space monitor, an advanced version of the Disk Space monitor, to monitor the amount of disk space that is currently in use on your server. This monitor enables you to:

- Monitor specific disks and counters on a host server using static counters. You can select one or multiple disks to monitor.
- Monitor changes in the host server's disks that correspond to a defined counter pattern. Dynamic monitoring enables you to configure the monitor once, and leave it to discover the addition and removal of disks and file systems in the environment and update itself.

When configuring a dynamic monitor, you can define a counter pattern that specifies the disks and counters you want to monitor. You can also define the required thresholds for the counter's pattern. The monitor scans the target host periodically, and creates the counters that are aligned with the given counter pattern.

If a new disk (or mount) is added to the machine and that disk corresponds to the counter pattern, the counters and thresholds that measure the disk are automatically added to the monitor when the counters are next updated from the server. Similarly, if a disk that corresponds to the counter pattern is no longer available, counters and thresholds for that disk are removed from the monitor (unless you choose not to delete them, in which case they are still displayed in the monitor's counter list).

For more details on the dynamic monitoring mechanism, see Dynamic Monitoring Mechanism in the Using SiteScope Guide.

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see ["How to Configure the HP NonStop Resources Monitor" on page 307](#).
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

## Monitor Run Frequency

The Dynamic Disk Space monitor does not require many resources, so you can run 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 in the Using SiteScope Guide.

**Note:** The frequency for updating counters from the server cannot be less than the monitor run frequency in Monitor Run Settings.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

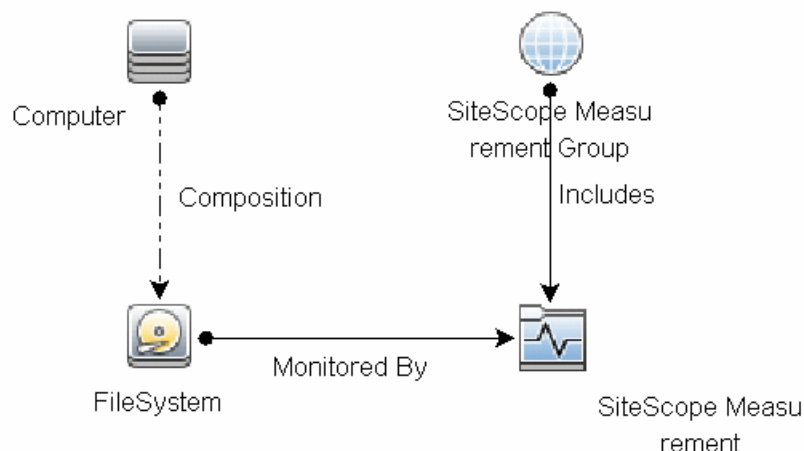
For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## Dynamic Disk Space Monitor Topology

The Dynamic Disk Space monitor can identify the topology of the server disks being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-base Usage
One point per disk  Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

# Tasks

## How to Configure the Dynamic Disk Space Monitor


### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- 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 -T <disk>`).

### 2. Configure the monitor properties

- a. Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **Dynamic Disk Space**. The New Dynamic Disk Space Monitor dialog box opens. For monitor user interface details, see ["Dynamic Disk Space Monitor Settings" on page 206](#).
- b. In the General Settings panel, enter a name and description for the monitor.
- c. In the Dynamic Disk Space Monitor Settings panel, select the server where the disk space you want to monitor is running.
- d. In the Counter Settings section, click the **Get Counter** button, and select the disk and counters you want to monitor from the Select Counters Form (the form displays static counters only). The counters are added to the Counter Preview tree.

**Tip:** The **Performance Counters Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Performance Counters Tool in the Using SiteScope Guide.

- e. The default counter patterns are displayed in the Patterns & Counters table. You can add other patterns to counters to instruct the monitor which counters to use. You can either:
  - Click the **Add New Counter**  button to add an empty line to the table, and create a pattern format using a regular expression. By default the following counters are created:

Counter Pattern	Description
./ */MB free/	Measures the amount of free memory.
./ */MB total/	Measures the total amount of memory.
./ */percent full/	Measures the percentage of the file system that is full.


**Tip:**

- (1). The pattern should always start and end with the forward slash ("/") character.
- (2). The "[" and "]" characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character).
- (3). Use "." to describe any character any number of times.

- Select a static counter, and edit the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.

**Example:**

If you enter the pattern `./ */. *platform. */MB free/`, the monitor retrieves the MB free counters on disks that contain the word platform in their file system's name.

- f. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counter Preview tree.
- g. Set the frequency for updating counters from the server in the **Frequency of updating counters from server** box. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.

- h. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful for keeping track of the counters that were previously being monitored.
- i. Click **Verify & Save** or **Save** to save your settings.
- j. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

**Note:** When configuring threshold settings for Dynamic Disk Space monitor:

- The monitor **always(default)** counter configured in the **Good if** section of the monitor's properties means that the state of the monitor is good, unless one of the thresholds of any of the other counters is breached.
- The **countersinError** counter configured in the **Error if** section of the monitor's properties means that the state of the monitor is error if one of the other counters is unavailable.

### 3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["Dynamic Disk Space Monitor Topology" on page 202](#).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

### 4. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the server where the disk space you want to monitor is running and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:




- The SiteScope **Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

## UI Descriptions

### Dynamic Disk Space Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>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></p> <ul style="list-style-type: none"> <li>Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li> <li>When working in template mode, 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> </ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p> <p><b>Note:</b> To avoid a timeout when monitoring a UNIX remote server using an SSH connection (if the external drives mounted by NFS are unavailable for the target remote), use the "umount -a -t nfs" command to unmount all NFS drives, or use "umount -n &lt;nodename&gt;" to unmount all the drives from the particular remote node that is unavailable. Use the "mount   grep nfs" command to get a list of NFS drives.</p>

UI Element	Description
<b>Counter Settings</b>	
<b>Get Counters</b>	Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.
<b>Patterns &amp; Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Click the <b>Add New Counter</b>  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the <b>Delete Counter</b>  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the <b>View Matches for Selected Pattern Counter</b>  button to display counters that match the selected patterns.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• SiteScope uses Perl regular expressions for pattern matching. For example, if you enter <code>/cpu.* /</code> or <code>cpu</code>, any counters with <code>cpu</code> in their name match this pattern and are added to the counters list.</li> <li>• To avoid error or null value in case the counter name contains "harddisk", replace the default regular expression with any of the following: <ul style="list-style-type: none"> <li>• <code>/^(?!.*Harddisk).*/MB free/</code></li> <li>• <code>/^(?!.*Harddisk).*/percent full/</code></li> <li>• <code>/^(?!.*Harddisk).*/MB total/</code></li> </ul> </li> </ul>
<b>Counter Preview</b>	Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.
<b>Frequency of updating counters from server</b>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p><b>Default value:</b> 1 hour</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The update frequency cannot be less than the monitor run frequency in Monitor Run Settings.</li> <li>• When configuring this setting in a template, the variable value can only be in time units of seconds.</li> <li>• Static counters are never deleted.</li> </ul>

UI Element	Description
<b>Continue displaying counters that no longer exist after update</b>	<p>When selected, counters that no longer exist after running the update mechanism to retrieve counters from the monitored server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful, for example, if a disk fails or for keeping track of counters that were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings on the next update.</p> <p><b>Default value:</b> Selected</p> <p><b>Note:</b> This option is relevant for dynamic counters only (those set using a regular expression). Static counters that are no longer available are still displayed even when this check box is cleared.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- This monitor supports setting fractional thresholds which are more useful than setting whole number thresholds when monitoring large disks (such as 1 terabyte and larger).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).

### Troubleshooting and Limitations

This section describes troubleshooting and limitations for Dynamic Disk Space monitors.

- ["Monitor does not send an individual alert for each disk space being monitored" below](#)
- ["Unable to retrieve disk information on a UNIX remote server" on the next page](#)
- ["WMI Returns Incorrect Disk Space Values" on the next page](#)
- ["Unable to get counters from Red Hat Enterprise Linux about network file systems" on the next page](#)
- ["Maximum Number of Counters That Can be Saved" on the next page](#)

**Monitor does not send an individual alert for each disk space being monitored**



If an error is encountered in one of the monitored disk spaces, the monitor status changes to Error and an alert is triggered. If another disk encounters an error, no additional notification is sent out because the monitor is already in Error status.

Workaround: Define a separate monitor for each disk. This way, an alert is triggered even if other disks (and monitors) are already in Error status.

### Unable to retrieve disk information on a UNIX remote server

When monitoring a UNIX remote server using an SSH connection, unable to retrieve disk information if the external drives mounted by NFS are unavailable for the target remote.

Workaround: Use the "umount -a -t nfs" command to unmount all NFS drives, or use "umount -n <nodename>" to unmount all the drives from the particular remote node that is unavailable. Use the "mount | grep nfs" command to get a list of NFS drives.

### WMI Returns Incorrect Disk Space Values

Due to a limitation with WMI, the WMI connection method returns incorrect results when this monitor is used on Windows Server 2008.

Workaround: To monitor Windows Server 2008 using WMI, install the Microsoft hot fix (<http://support.microsoft.com/kb/961435/en-us>) on the target Windows system.

### Unable to get counters from Red Hat Enterprise Linux about network file systems

By default, SiteScope is only able to display file systems under /dev. To change this, do the following:

1. Create a backup of the **<SiteScope root directory>/templates.os/Linux.config** and **<SiteScope root directory>/templates.os/RedHatEnterpriseLinux.config** files.
2. Edit the **<SiteScope root directory>/templates.os/Linux.config** as follows:
  - Search for "id=disks".
  - Add the following to the bottom of the "id=disks" section (the lines between the #s define each section):

```
noNameFilter=true
startLine=2
#
```
  - Save the file.
3. Repeat for the **<SiteScope root directory>/templates.os/RedHatEnterpriseLinux.config** file.
4. Restart SiteScope.

### Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the **\_browsableContentMaxCounters** parameter in the **master.config** file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the **\_maxCountersForRegexMatch** parameter in the **master.config** file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The **\_maxCountersForRegexMatch** parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both **\_browsableContentMaxCounters** and **\_maxCountersForRegexMatch** parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

## Troubleshooting Logs

1. Check for dynamic framework errors in:

- **<SiteScope root directory>\logs\dynamic\_monitoring\_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
- **<SiteScope root directory>\logs\dynamic\_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).

To check for dynamic monitoring errors, copy the following section from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####  
# Dynamic Monitoring  
#####  
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=  
DEBUG, dynamic.monitoring.appender  
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=false  
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG, dynamic.monitoring.appender  
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false  
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFileAppender  
log4j.appender.dynamic.monitoring.appender.File=./${log.file.path}/dynamic_monitoring.log  
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB  
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5  
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.PatternLayout  
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
```

2. Check for Dynamic Disk Space monitor errors in:

- **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.

# Chapter 28: Dynamic Docker Monitor

The Dynamic Docker monitor enables you to monitor the health and performance statistics of a Docker environment, from the cluster manager level through the Docker daemon layer, to the container level and applications which run inside the containers. It also monitors the health of the cluster manager and each Docker node. You can choose to monitor a single Docker node, a full cluster, or several nodes on a cluster.

After selecting the measurements you want to monitor, the dynamic monitoring mechanism automatically update counters and thresholds that changed during run-time on Docker nodes and clusters. The Dynamic Docker monitor also includes a mechanism that enables it to discover applications running in new containers detected on the Docker node or cluster, and to automatically create a monitor, or set of monitors, for each new application. The monitor automatically retrieves metrics for every new container that is created on the node or

cluster and adds them to the monitor. Similarly, if a container is removed, metrics for that container are automatically removed from the monitor. Dynamic monitoring enables you to configure the monitor on a one time basis, and leave it to update itself.

Using the Unified Console in SiteScope, you can see a consolidated view of all monitored Docker metrics at the same level in a flattened view as a set of nested rectangles. The hierarchical relationship between the data is retained, enabling drill down/up to different levels.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Dynamic Docker monitor.

# Learn About

This section includes:

- ["Dynamic Docker Monitor Overview" below](#)
- ["Docker Counters" on the next page](#)
- ["SSL Connectivity" on the next page](#)
- ["Supported Platforms/Versions" on page 213](#)
- ["License Consumption" on page 213](#)

## Dynamic Docker Monitor Overview

Docker is an open source container technology that uses containers to wrap software in a complete file system that contains everything it needs to run. These containers use shared operating systems on top of a single machine, making disk usage and image downloads much more efficient.

### Dynamic Monitoring

The SiteScope Dynamic Docker monitor enables you to monitor specific Docker containers and counters on defined Docker nodes, or on a cluster. During initial monitor creation, the monitor scans the target Docker node or cluster to dynamically discover the hierarchy and available performance counters. You can select from these performance counters to determine which measurements SiteScope should retrieve for reporting server status. You can also define the required thresholds for the counter's pattern. In this way, thresholds are also updated automatically when the counters are updated.

For details on configuring the Dynamic Docker monitor, see ["Dynamic Docker Monitor" on the previous page](#).

### Automatic Discovery Mechanism

The Dynamic Docker monitor also includes a mechanism that enables it to discover applications running in new containers detected on the Docker node or cluster, and to automatically create a monitor or set of monitors for each new application. For each application type, you need to create a unique config file (for example, one for Tomcat and another for MySQL, Postgres, and so forth), and a template to deploy a monitor or set of monitors for each container application that you want to monitor.

Each time the monitor requests counters from the server (according to the **Frequency of updating counters from server** value), the discovery mechanism checks the list of containers supplied by the monitor and searches for a config file that matches the container image. If it finds a matching config file, it automatically creates and deploys a new monitor or set of monitors for each application using a predefined template (listed in the config file).

For details on configuring the discovery mechanism, see ["How to Configure Automatic Docker Application Discovery" on page 218](#).

### Monitor Run

Dynamic monitors automatically adjust the SiteScope monitoring configuration based on changes that are happening in your IT environment. When the monitor runs, it accesses the Docker node or the cluster API, checks its availability, collects health counters and specific metrics on the Linux host for every registered Docker node and on the Docker daemon.

If automatic discovery is enabled, the monitor also activates a process which deploys a template (containing a new monitor or set of monitors) on the application level, for applications detected on the node or cluster. It also removes the deployed application monitors and counters when a container is removed. This enables you to configure the monitor one time, and leave it to automatically discover changes in the environment and update itself.

The Dynamic Docker monitor monitors running containers. If a container stops running or is deleted from the Docker, the monitor stops monitoring the container, unless **Continue displaying counters that no longer exist after update** is selected, in which case, the container's counters are displayed as unavailable. If a container stops running, the group that was deployed to monitor it is disabled; it is enabled once the container continues to run again. If a container is deleted, the group that was deployed to monitor it is also deleted. These actions take affect each time counters are requested from the server according to the **Frequency of updating counters from server** value set for the monitor.

**Note:** If the server is changed to another Docker node, all the deployed application groups are deleted.

### Docker Counters

The following counter types are available on the Dynamic Docker monitor:

- Cluster and Docker Node Counters for measuring availability and performance of Daemon counters on the Docker cluster manager and Docker nodes.
- Container Counters for measuring the health of each of the containers on the Docker nodes.
- Health Counters (CPU, memory, and disk space) for measuring the performance and operational health of the cluster manager and each Docker node. Health counters for Docker nodes are only displayed if a remote server has been configured on the Docker node.

These counters are displayed in the Counters tree after connecting to the remote server of the Docker node or cluster machine to be monitored. For the list of counters, see ["Monitor Counters" on page 231](#).

### SSL Connectivity

The Docker REST APIs are generally configured to use SSL encryption to protect the Docker API endpoint from unauthorized access. Monitoring a Docker that uses an encrypted connection requires you to import the server certificate. 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 ["Dynamic Docker Monitor" on page 210](#).
- Importing the server certificate. For details on how to perform this task, see ["How to Configure the Dynamic Docker Monitor" on the next page](#).

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol/HTTP Client used by SiteScope	Java ("Use WinInet" is not selected)	WinInet ("Use WinInet" is selected)
SSLv2	x	x
SSLv3	√	√
TLSv1.0, TLSv1.1, TLSv1.2	√	√

## Supported Platforms/Versions

- This monitor supports monitoring Docker version 1.x (the latest certified version is Docker 1.9.0).
- This monitor supports Dockers running on Linux operating systems only.
- This monitor supports Docker Swarm (a Docker-native clustering system) for monitoring a cluster of Docker containers.
- This monitor supports Docker Kubernetes for monitoring a cluster of Docker containers.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per Docker in a cluster	One OS instance license per monitored host and one OS instance license for each monitored virtual machine. As a result, OSi capacity consumption for Dynamic Docker monitors can change during the monitor run according to the number of discovered VMs.

# Tasks

## How to Configure the Dynamic Docker Monitor

### 1. Prerequisites

- You must configure a UNIX remote server for each Docker cluster and node that you want to monitor. Health counters for Docker nodes are only displayed if a remote server has been configured on the Docker node.

For details, see [Configure SiteScope to Monitor Remote UNIX Servers](#) in the [Using SiteScope Guide](#).

**Tip:** When configuring the remote server name in the **Server** field of the UNIX Remote Server dialog box, you should use the same name that is configured in the Docker or cluster. For example, if the Docker uses an IP address to identify the server, then an IP address should be used in the remote server name.

- If you want to monitor a Swarm cluster or a Docker node directly, make sure the REST API is open to the SiteScope machine (you will need to specify the port when creating the monitor below).

- If you want to monitor a Kubernetes cluster, install cAdvisor on the Kubernetes machine and open both the Kubernetes REST API and the cAdvisor port to the SiteScope machine (you will need to specify the ports when creating the monitor below).
- If you plan on using automatic application discovery to have SiteScope search for new Docker applications and automatically create new application monitors using predefined templates, follow the steps in ["How to Configure Automatic Docker Application Discovery" on page 218](#).
- Performance
  - To avoid unnecessarily monitoring containers (those that are dropped after a short period of time), containers must be running for a minimum amount of time before they are monitored. By default, containers must be running for a minimum of one minute. You can change the minimum running period for containers in the **\_DockerMinimumContainerRunningTimeInMinute** property in the **<SiteScope root directory>\groups\master.config** file. Note that the monitor will not monitor containers that run for less the configured time.
  - You can configure the number of threads for the monitor run using the parameter **\_dynamicDockerCheckContainersStatsThreadPullSize**. Each thread handles a set of containers on the Docker cluster/daemon. The parameter is available in the master.config file (**<SiteScope root directory>\groups\master.config**). Default value of the parameter is 15 threads.
  - For faster performance, you can exclude monitoring the health of the cluster or docker node. It is recommended that you use other SiteScope monitors such as Dynamic Disk Space/CPU/Memory monitors to monitor the health of the docker node or cluster.
- If you plan to connect to the remote server using a secure connection, the user name and password specified in the Credentials section (in Authentication Settings) must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.


## 2. Import the server certificates (if the Docker server is configured to use SSL encryption)

If the Docker REST API is configured to use SSL encryption, then 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 [How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide](#).
- Import the server certificates manually. For details, see ["How to Manually Import Server Certificates " on page 224](#).

## 3. Configure the monitor properties

- a. Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **Dynamic Docker**. The New Dynamic Docker Monitor dialog box opens.
- b. In the General Settings panel, enter a name and description for the monitor.
- c. In the Dynamic Docker Monitor Settings panel, configure the monitor properties as required. For a description of each setting, see the [Main Settings UI descriptions](#).
- d. In the **Patterns & Counter** section, click the **Get Counter** button, and select the relevant counters you want to monitor on the Docker cluster or node (the form displays static counters only). The counters are added to the Counter Preview tree. You can click the **Reload Objects** button to reload data for the selected cluster or node.

- e. The default counter patterns are displayed in the Patterns & Counters table. You can add other patterns to counters to instruct the monitor which counters to use. You can either:
- Click the **Add New Counter**  button to add an empty line to the table, and create a pattern format using a regular expression, or you can use the following out-of-the box regular expressions that are created by default:

Counter Pattern	Description
././memory%/	Measures the total amount of free memory (in percentage).
././cpu usage/	Measures the CPU usage.
././disk usage I/O write \(\bytes\)	Measures the disk usage in bytes.
././state/	Checks the state of the Docker container.
././network usage transmitted/	Measures the network usage (transmitted data).
././network usage received/	Measures the network usage (received data).
././availability/	Checks the availability of the Docker container.
././disk usage I/O read \(\bytes\)	Measures the disk usage in bytes.

**Tip:**

- The pattern should always start and end with the forward slash ("/") character.
- Special characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character).
- Use ".\*" to describe any character any number of times.

**Example:** ./.\cpu usage%/ , shows CPU usage for all the currently running containers on the Dockers connected to Swarm that you are monitoring.

If you have two virtual machines (Docker 1 and Docker 2), this pattern finds for the Docker:


```
Swarm1/Docker1/Health Counters/CPU/.*
Swarm1/Docker2/Health Counters/CPU/.*
```

and for the containers on Docker1 connected to Swarm1:

```
Swarm1/Docker1/Container1/cpu usage%
Swarm1/Docker1/Container2/cpu usage%
```

- Select a static counter, and edit the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions in the Using SiteScope Guide.

**Note:** For details on the maximum number of counters that can be selected from the browsable tree and the maximum number of counters that can match the selected counter patterns when creating and updating dynamic monitors, see ["Tips/Troubleshooting" on page 232](#). If the maximum number of counters that can be deployed is exceeded, an error is written to the **RunMonitor.log**.

- f. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counter Preview tree.

- g. You can change the frequency for updating counters from the server in the **Frequency of updating counters from server** box (the default value is one hour). This determines the time interval at which counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches.

Tip: For obtaining more up-to-date data with the Docker monitors, the suggested value for **Frequency of updating counters from server** and the monitor frequency is 1 minute (60 seconds) or higher.

The monitor also checks the list of containers that was supplied by the monitor and searches for new containers. If it finds a new container monitored by the Docker monitor, it searches the container for known applications (ones that have been matched to a config file in **<SiteScope root directory>\templates.docker\applications**), and it automatically creates and deploys a new monitor or set of monitors for the applications using predefined templates (mentioned in the config file). The monitor deploys a new template for every new container that is created on the node or cluster, and removes the deployed monitors and counters when a container is removed.

**Note:**

- Each application type that has a different template should have a unique config file (for example, one for Tomcat and another for mySQL Postgres, and so forth).
- If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.

- h. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful for keeping track of the counters that were previously being monitored.

**Note:** When using this option, application groups are deleted only when the Check Containers Still Exist schedule is activated. For details on schedulers, see ["How to Configure the Automatic Discovery Mechanism Schedulers"](#) on page 221.

For details on the counters and patterns settings, see [Dynamic Docker Counter Settings](#).

- i. If you want to enable SiteScope to connect to the Docker nodes using a secure connection, select **Enable secure connection**, and configure the proxy and authentication settings as required. See the [proxy](#) and [authentication](#) UI settings for details.

Tip: Common case scenario is to use the TLS protocol for the Docker REST API communication. To use TLS, you have to import your CA certificate into SiteScope (Preferences > Certificates). Copy the client certificate and key (PFX file) into the directory **<SiteScope\_Dir>/SiteScope/templates.certificates** on your SiteScope system. In the **Authentication Settings** pane, select the certificate file in the **Client Side certificate** and enter password, if any. Choose the option **Prefer TLS to SSL** from the list of **Preferred Protocols**. See the [Authentication Settings](#) for more details.

- j. Click **Verify & Save** or **Save** to save your settings.
- k. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance, or use the out-of-the box threshold settings. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.



For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

**Note:** When configuring threshold settings for Dynamic Docker monitor:

- The monitor **always(default)** counter configured in the **Good if** section of the monitor's properties means that the state of the monitor is good, unless one of the thresholds of any of the other counters is breached.
- The **countersinError** counter configured in the **Error if** section of the monitor's properties means that the state of the monitor is error if one of the other counters is unavailable.

#### 4. Results

During each update, the monitor connects to the server where the Docker or cluster manager and its connected Dockers are running, and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

If a new Docker or container is added to the cluster or Docker, the monitor retrieves the list of counters from the cluster or Docker (which also contains the new added container). If the new Docker or container contains counters that correspond to any of the defined counter patterns, these counters are added to the counter list.

If you enabled automatic application discovery, the monitor searches for new containers. If it finds a new container, it searches the container for known applications (ones that have been matched to a config file on **<SiteScope root directory>\templates.docker**), and it automatically creates and deploys a new monitor or set of monitors for the application using a predefined template. The new monitors automatically retrieve metrics for every new container.

**Note:** Application groups created by the discovery mechanism are automatically deleted by the Dynamic Docker monitor in the following cases:

- a. If the main Dynamic Docker monitor was deleted, provided **Dynamic Docker: Delete monitors created by discovery mechanism when Docker monitor deleted** is selected in **Preferences > Infrastructure Preferences > Monitor Settings**. If this setting is cleared, only the Dynamic Docker monitor is deleted; the discovered application groups remain.
- b. If the Docker node was disconnected from the cluster in which it is monitored.
- c. If all the counters on one of the containers were removed from the Dynamic Docker monitor.
- d. If the server of the Docker monitor was changes to a different remote server that represents a different Docker node.

#### 5. Troubleshoot / Check Monitor Performance (if required)

- You can use the log files to troubleshoot monitor and automatic discovery issues. For information on troubleshooting the Dynamic Docker monitor see ["Troubleshooting Dynamic Docker Monitor Logs" on page 233](#). For information on troubleshooting the application discovery mechanism, see ["Troubleshooting Dynamic Docker Application Discovery Logs" on page 233](#).
- You can check the performance of the dynamic monitoring framework in:
  - The SiteScope **Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Monitor in the Using SiteScope Guide.
  - In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

## 6. Delete Dynamic Docker / Auto Discovery Application Monitors (if required)

You can delete the application monitors at any time without restrictions.

When deleting the Dynamic Docker monitor, the application monitors dependent on the Docker monitor are also deleted provided **Dynamic Docker: Delete monitors created by discovery mechanism when Docker monitor deleted** is selected in **Preference > Infrastructure Preferences > Monitor Settings** (it is selected by default). If this setting is cleared, only the Dynamic Docker monitor is deleted and the application monitors remain.

**Note:** You cannot delete the Dynamic Docker monitor if other monitors depend on it without first removing the dependency.

## How to Configure Automatic Docker Application Discovery

### 1. Prerequisites.

For each Docker node or cluster application you want to monitor, make sure that a public facing port is associated with each application you want to monitor.

### 2. Enable the Dynamic Docker application discovery mechanism in Infrastructure Preferences.

In **Preference > Infrastructure Preferences > Monitor Settings**, make sure that **Dynamic Docker: Enable automatic application discovery** is selected (it is selected by default).

**Note:** You must restart SiteScope if you change this setting.

### 3. Configure the other Dynamic Docker application discovery settings - optional

- To automatically delete application monitors created by the automatic discovery mechanism when deleting a Dynamic Docker monitor, make sure that **Dynamic Docker: Delete monitors created by discovery mechanism when Docker monitor deleted** is selected in **Preference > Infrastructure Preferences > Monitor Settings** (it is selected by default).
- To avoid unnecessarily monitoring containers (those that are dropped after a short period of time), containers must be running for a minimum amount of time before they are monitored. By default, containers must be running for a minimum of one minute. You can change the minimum running period for containers in the `_DockerMinimumContainerRunningTimeInMinute` property in the `<SiteScope root directory>\groups\master.config` file.

### 4. Configure the scheduler parameters that are used by the automatic discovery mechanism - optional

You can fine tune the scheduler parameters used by the automatic discovery mechanism in the `<SiteScope root directory>\groups\master.config` file. For parameter details, see ["How to Configure the Automatic Discovery Mechanism Schedulers"](#) on page 221.

### 5. Navigate to the `<SiteScope root directory>\examples\monitors\dynamic_docker_monitor` folder, and extract the contents of the `TomcatOnDockerExample.zip` file to a location of your choice. The zip file contains an example template and config file to help you set up application discovery.

### 6. Create a template for each application you want to monitor on the Docker nodes.

To automatically monitor container applications running on the Docker node, you can use the example template as described below (the recommended method), or you can create a new template as described in [Create Templates in the Using SiteScope Guide](#).

- a. In SiteScope, select the **Templates** context.
- b. In the template tree, right-click the **SiteScope** root container, and select **Import > Template**.
- c. Navigate to the example Dynamic Docker files you downloaded, and select the **DockerizedTomcatApplicationTemplate** file.
- d. After importing the template, modify the template objects as required to suit your monitoring requirements.

**Tip:** You can test the template by deploying it manually on the container application and making sure the template objects are added to the monitor tree.

7. Create a unique config file for each application type you want to monitor. For example, one for Tomcat and another for mySQL Postgres, and so forth.

The config file is used to automatically deploy a monitor or set of monitors (from the template created in the previous step) for each container application that you want to monitor on the Docker nodes.

- a. Navigate to the sample Dynamic Docker files you downloaded, and open the **Tomcat.config** file.
- b. Edit the file to meet your configuration needs by following the instructions and using the examples supplied in the file.

The file includes the following:

- A regular expression to match the container applications you want to monitor (`app_pattern_identifier`). The regular expression in the config file should be matched to the container image.

**Note:**

- Use an appropriate regular expression to ensure that each container image is matched to only one config file. If more than one config file is matched to the same container image, one of the config files will be chosen at random.
- If you plan on deploying several monitors on the same Docker application, each group path name should be unique. You can do this by using an identifying variable in the group path name (as in the example on the example **Tomcat.config** file), or change the root group name on the template to be unique (as in the template example (**DockerizedTomcatApplicationTemplate**)).

- (optional) A regular expression to match the container name (`container_name_pattern_identifier`).

**Note:** The `container_name_pattern_identifier` key is an option to specify the config file containers in addition to the `app_pattern_identifier`. If this value is not specified, then a general regular expression such as `.*` is used as the key value.

- The path to the template that will be deployed (`template_full_path`). You can use the following keys (taken from the Docker and container data) in the template path:

`<CLUSTER_SERVER_NAME>, <DOCKER_SERVER_NAME>, <IMAGE_NAME>, <CONTAINER_NAME>, <CONTAINER_ID>, <APP_EXPOSED_PORT>`

For a Kubernetes cluster, you can use the following keys:

`<CLUSTER_KUBERNETES_POD_NAME>, <CLUSTER_KUBERNETES_POD_ID>, <CLUSTER_KUBERNETES_NAMESPACE_NAME>`

- (Optional) The path to the target group in the deployed template (`target_group_full_path`).
- The internal port and type for the container application (`internal_port_binding_key`).

- The template variables required to deploy the template. You can use known keys for the templates variables as:

<CLUSTER\_SERVER\_NAME>, <DOCKER\_SERVER\_NAME>, <IMAGE\_NAME>, <CONTAINER\_NAME>, <CONTAINER\_ID>, <APP\_EXPOSED\_PORT>

For Kubernetes cluster, you can use:

<CLUSTER\_KUBERNETES\_POD\_NAME>, <CLUSTER\_KUBERNETES\_POD\_ID>, <CLUSTER\_KUBERNETES\_NAMESPACE\_NAME>

- c. Save the config file with an appropriate name, and copy it to the **<SiteScope root directory>\templates.docker\applications** folder (it must have the .config extension).
8. When configuring the monitor settings (in the previous task), for each Dynamic Docker monitor on which you want to use automatic application discovery, make sure **Enable automatic application discovery** is selected (this is the default setting).

You can also modify the time interval used by the monitor for retrieving and updating counters from the server in the **Frequency of updating counters from server** box. During the interval, the application discovery mechanism searches for newly monitored or deleted containers, existing containers which stop or are restarted, and it adds/removes/disables/enables (respectively) the application group according to the config files.

For details of UI settings, see ["Dynamic Docker Monitor" on page 210](#).

## How to Configure the Automatic Discovery Mechanism Schedulers

The Dynamic Docker monitor includes scheduler parameters that you can use to tune the automatic discovery mechanism.

You configure these parameters in the **<SiteScope root directory>\groups\master.config** file:

Scheduler	Parameter Name / Description
Redeploy / Publish Templates Due to Config File Changes	<p><b>Parameter:</b> <code>_dynamicDockerAppDiscoverReDeployTemplatesRateDueToConfigFileChangesInMinutes</code></p> <p><b>Description:</b> Amount of time, in minutes, to wait between checking whether the config files were updated. If config files were updated, the discovery mechanism searches for all groups that were deployed by the config files and attempts to redeploy templates or publish template changes.</p> <p><b>Differences between types of changes:</b></p> <ul style="list-style-type: none"> <li>• If the <code>internal_port_binding_key</code> variable or one of the template variables changes, the scheduler tries to publish this change to all groups that were deployed by the template.</li> <li>• If the template itself changes (<code>template_full_path</code>), the scheduler deletes all groups that were deployed by the template and tries to redeploy the template.</li> <li>• If the path to the target group in the deployed template (<code>target_group_full_path</code>) changes, nothing happens to previously deployed groups, but a new group will be deployed to the new path.</li> </ul> <p><b>What happens if redeployment or publish changes fails?</b></p> <ul style="list-style-type: none"> <li>• When redeploying the template, the mechanism deletes the previous group and attempts to redeploy the template on this container the number of times specified in the <code>_dynamicDockerAppDiscoverDeployTemplateAttempts</code> parameter. The frequency of attempts is determine by the value in the <code>_dynamicDockerAppDiscoverDeployTemplateRetriesRateInMinutes</code> scheduler below.</li> <li>• When publishing template changes, the mechanism attempts to publish the template on this container the number of times specified in the <code>_dynamicDockerAppDiscoverDeployTemplateAttempts</code> parameter. If all attempts fail, the previously deployed group will remain unchanged.</li> </ul> <p>If all attempts to redeploy or publish the template fail, the container is removed from the waiting list.</p> <p><b>Default Value:</b> 15 minutes (minimum value is 5 minutes)</p>

Scheduler	Parameter Name / Description
Retry Template Deployment / Publishing	<p><b>Parameter:</b> <code>_dynamicDockerAppDiscoverDeployTemplateRetriesRateInMinutes</code></p> <p><b>Description:</b> Amount of time, in minutes, to wait before attempting to deploy template or publish template changes after the previous attempt failed.</p> <p><b>Possible reasons for templates failing to deploy:</b></p> <ol style="list-style-type: none"> <li>1. There is no matched config file for the container image.</li> <li>2. The container is not running.</li> <li>3. There are no exposed ports on the container. This will occur, for example, if the user used the <code>&lt;APP_EXPOSED_PORT&gt;</code> key on the config file.</li> <li>4. The discovery mechanism fails to find the <code>internal_port_binding_key</code> in the container internal ports list that was selected in the config file.</li> <li>5. Unable to find the template from the <code>template_full_path</code> in the config file.</li> <li>6. Template variables are incorrect (key or value) in the config file.</li> <li>7. Template deployment failed for some specific reason.</li> </ol> <p>The mechanism attempts to deploy the template on this container the number of times specified in the <code>_dynamicDockerAppDiscoverDeployTemplateAttempts</code> parameter. If all attempts fail, the container is removed from the waiting list.</p> <p><b>Default Value:</b> 30 minutes (minimum value is 5 minutes)</p>
Check Containers Still Exist	<p><b>Parameter:</b> <code>_dynamicDockerAppDiscoverCheckContainersExistencesRateInMinutes</code></p> <p><b>Description:</b> Amount of time, in minutes, to wait before checking for the state of groups that were deployed on containers that are stopped/restarted/deleted. When a container is stopped/restarted/deleted, the discovery mechanism automatically disables/enables/deletes any groups that are deployed on the container.</p> <p><b>Default Value:</b> 1440 minutes (24 hours). The minimum value is 5 minutes.</p>

The `<SiteScope root directory>\groups\master.config` file also includes the following additional discovery mechanism parameters that influence the schedulers:

- **`_dynamicDockerAppDiscoverConfigFilesSampleRateInSeconds`**. Frequency, in seconds, for checking the config file directory for changes. The default value is 30 seconds (minimum value is 30 seconds). If a new config file is added, or an existing file is deleted, the config file list is updated.
  - If a config file is modified by updating the container identifiers (`app_pattern_idenfier` and `container_name_pattern_idenfier`), the config file is considered a new file.
  - If a config file is modified by changing the `internal_port_binding_key`, or the template variables, the file is marked to be published, and is handled according to the `_dynamicDockerAppDiscoverReDeployTemplatesRateDueToConfigFileChangesInMinutes` scheduler.
  - If a config file is modified by changing the template path (`template_full_path`), the file is marked to be redeployed, and is handled according to the `_dynamicDockerAppDiscoverReDeployTemplatesRateDueToConfigFileChangesInMinutes` scheduler.

- If a config file is modified by changing the group path (`target_group_full_path`), nothing happens to previously deployed groups, but a new group will be deployed to the new path.
- If a config file is deleted, groups that were previously deployed according to this config file are not deleted, but new containers which arrive will fail due to the config file for their image no longer existing.
- **\_dynamicDockerAppDiscoverDeployTemplateAttempts**. The number of attempts to redeploy templates or publish template changes on some container. This variable influences the **\_dynamicDockerAppDiscoverReDeployTemplatesRateDueToConfigFileChangesInMinutes** and **\_dynamicDockerAppDiscoverDeployTemplateRetriesRateInMinutes** schedulers. The default value is 3 attempts (minimum 1 attempt).
- **\_dynamicDockerAppDiscoverThreadPullSize**. Amount of thread handlers that handle Docker monitor deletion, application group deletion, and docker monitor configuration updates from Dynamic Docker monitors. The default value is 25 thread handlers (minimum 1 thread handler).

For achieving better performance, it is recommended to keep this value roughly equal to the result of the formula –  $((\text{Number of Docker nodes to be monitored}) * 10) / (\text{frequency of updating counters from server in minutes})$ . For example, if number of Docker nodes is 20, update counter frequency is desired to be set to 5 minutes, then the value of this parameter should be  $((20 * 10) / 5) = 40$ .

- **\_dynamicDockerAppDiscoverMaxNumberOfContainersPerThread**. Number of containers handled by 1 thread. That is, if an update was made on the Docker like new containers being created or if existing containers were stopped, deleted, or started (if already stopped) which influence the Docker monitor counters list during the process of updating the counters list from the server. The default value is 50 containers per thread. (Minimum value is 1 container per thread).

For achieving better performance, it is suggested to keep this value as equal to the maximum number of containers expected to run on any of the Docker nodes to be monitored using SiteScope.

**Tip:** To improve application discovery performance, we recommend increasing the number of handlers and decreasing the number of counters per thread. In addition, you can separate the Docker containers between several monitors. You can separate the containers to several groups by using the regular expression field.

Examples regular expressions to separate containers into groups:

- Use `/Cluster/host1/Containers/*/` to monitor all containers on a specific host.
- Use `/Cluster/host1/Containers/jdk*/` to monitor all containers on a specific host with a name starting with 'jdk'.

### How to Implement Changes Immediately Using JConsole

If you made changes to a config file and you want these changes to take effect without waiting for the scheduler, you can use JConsole to implement these changes immediately. You can also use JConsole to check scheduler progress.

1. To access the JConsole tool, run **<SiteScope root directory>/java/bin/jconsole** binary file on UNIX platforms.
2. Depending on which SiteScope you want to monitor, select **Local Process**, or **Remote Process** with port **28006** (the default JMX port).
3. Select the **MBeans** tab, and open **com.mercury.sitescope/Core/Platform/Monitors/DynamicDockerJmxMBean**. To check scheduler

progress, select the relevant scheduler under **Attributes** and click the scheduler refresh button. To run a scheduler, select the relevant scheduler under **Operations** and click the invoke scheduler button.

## How to Manually Import Server Certificates

Instead of using Certificate Management, you can manually import certificates 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 in the Using SiteScope Guide.

1. Check the certificates already in the keystore, from the **<SiteScope root directory>\javallib\security** directory, by entering:

```
../../bin/keytool -list -keystore cacerts
```

2. Import the certificate, into **<SiteScope root directory>\javallib\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.

## How to View Docker Counters and Application Groups/Monitors in the Unified Console

1. Prerequisites

The groups displayed in the Unified Console are those that can be accessed by the user profile logged on to SiteScope. Similarly, the actions that can be performed on groups and monitors are dependent on the action permissions assigned to the user account. For details on user accounts, see User Management Preferences.

2. Open Multi-View or Ops View in the Unified Console.

- In a Web browser, enter:

`http://<server_name>:<port>/SiteScope/WebMain#/multiview` for Multi-View, or

`http://<Server_name>:<port>/SiteScope/WebMain#/consolidatedview` for Ops View.

- From the SiteScope Dashboard: Select the **Monitors** context, click the **Dashboard** tab, and then click the **Unified Console** button. The Unified Console opens in Ops View, which displays both Multi-View and the Event Console. To display only Multi-View, click **Multi-View**.

3. To display a consolidated view of all Docker containers being monitored:

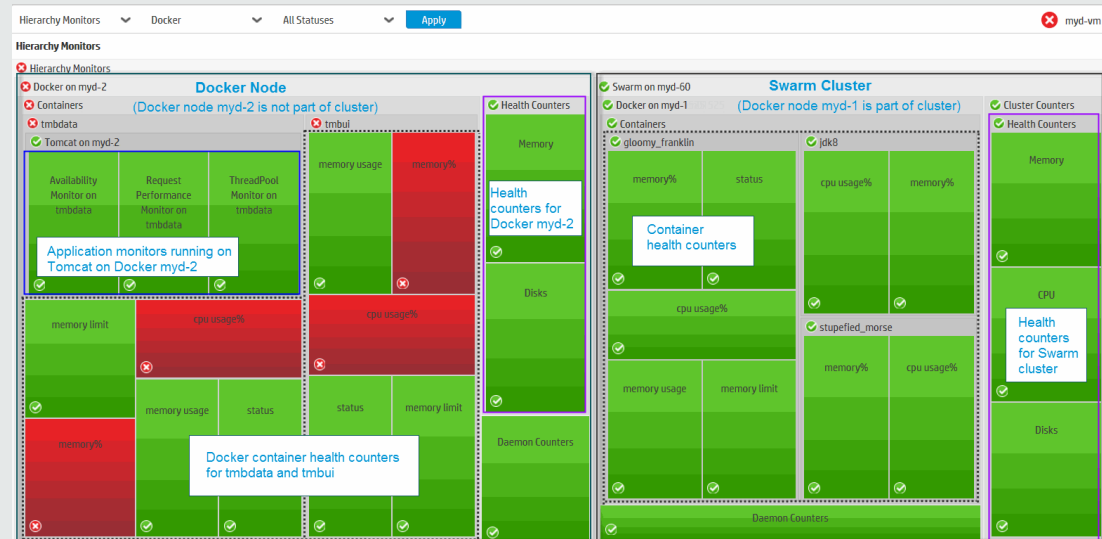
- a. In Multi-View/Ops View, click the arrow next to the drop-down list on the upper left side of the window, and select **Hierarchy Monitors**. The name in the adjacent drop-down list changes to



## Docker.

- b. Click **Apply**. SiteScope displays all Dynamic Docker monitors at the same level. It includes the Docker cluster manager (if selected for monitoring), all Docker nodes, container groups with application monitors, Daemon counters, and Health Counters in a flattened view as a set of nested rectangles. The hierarchical relationship between the data is retained, enabling drill down/up to different levels.

**Example:** Multi-View showing all Dynamic Docker monitors that are being monitored at the root level



- c. In addition, you can filter items in the Hierarchy tree according to their status (Good, Warning, or Error) using the Status filter.




For more details on using the Unified Console, see [How to Select and Configure a View in the Using SiteScope Guide](#).

## UI Descriptions

### Dynamic Docker Monitor Settings

User interface elements are described below:

Main Settings	
UI Element	Description
<b>Server</b>	<p>Name of the server where the Docker cluster or node you want to monitor is running. Select a server from the server list (only those UNIX remote servers that have been configured in SiteScope are displayed), or click the <b>Add Remote Server</b> to add a new UNIX server.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>When configuring this monitor on SiteScopes running on UNIX versions, only remote servers that have been configured with an SSH connection method are displayed. For details, see Configure SiteScope to Monitor Remote UNIX Servers in the Using SiteScope Guide.</li> <li>When working in template mode, 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> </ul>
<b>Add Remote Server</b>	Opens the Add UNIX Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.
<b>Cluster</b>	Select to monitor all Dockers in the cluster. Select the cluster type <b>Swarm</b> or <b>Kubernetes</b> from the drop-down list.
<b>Docker</b>	Select to monitor a specific Docker node.
<b>Port</b>	<p>API port for the selected cluster or Docker node.</p> <p><b>Note:</b> If you want to monitor a cluster or a Docker node directly, make sure the REST API is open to the SiteScope machine.</p>
<b>cAdvisor Port</b>	If you selected the cluster type as Kubernetes, enter the cAdvisor API port for the Docker Kubernetes cluster.
<b>Enable automatic application discovery</b>	<p>Select to use the discovery mechanism to search for applications running in new containers on the Docker node or cluster, and to automatically create a new monitor or set of monitors for each application detected (provided the application is matched to some config file) using a predefined template.</p> <p><b>Note:</b> This check box is inactive if the global application discovery setting <b>Dynamic Docker: Enable automatic application discovery</b> has been disabled in <b>Preference &gt; Infrastructure Preferences &gt; Monitor Settings</b> (it is selected by default).</p>

Main Settings	
UI Element	Description
<b>Monitor all containers</b>	<p>Monitors all containers irrespective of their state. If unchecked, only running containers are monitored.</p> <p>Default value: Selected</p>
Counter Settings	
<b>Get Counters</b>	<p>Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.</p> <p>For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on page 231</a>.</p>
<b>Patterns &amp; Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Click the <b>Add New Counter</b>  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the <b>Delete Counter</b>  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the <b>View Matches for Selected Pattern Counter</b>  button to display counters that match the selected patterns.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• SiteScope uses Perl regular expressions for pattern matching. For example, if you enter <code>/cpu.*/</code> or <code>cpu</code>, any counters with <code>cpu</code> in their name match this pattern and are added to the counters list.</li> <li>• By default, when creating a Docker monitor there are out-of-the box Thresholds Settings for the default <code>./*/memory%/</code> and <code>./ */cpu usage%/</code> counters.</li> <li>• By default, the following regular expressions are available: <ul style="list-style-type: none"> <li>• <code>./*/disk usage I\O write \(\bytes\)</code></li> <li>• <code>./*/state</code></li> <li>• <code>./*/network usage transmitted/</code></li> <li>• <code>./*/network usage received/</code></li> <li>• <code>./*/availability/</code></li> <li>• <code>./*/disk usage I\O read \(\bytes\)/</code></li> </ul> </li> </ul>
<b>Counter Preview</b>	<p>Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.</p>

Main Settings	
UI Element	Description
<b>Frequency of updating counters from server</b>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p>Tip: For obtaining more up-to-date data with the Docker monitors, the suggested value for <b>Frequency of updating counters from server</b> is 1 minute (60 seconds) or higher.</p> <p><b>Default value:</b> 1 hour</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>The update frequency cannot be less than the monitor run frequency in Monitor Run Settings.</li> <li>When configuring this setting in a template, the variable value can only be in time units of seconds.</li> <li>Static counters are never deleted.</li> </ul> <p>For more details, see <a href="#">"Dynamic Docker Monitor Overview" on page 211</a>.</p>
<b>Continue displaying counters that no longer exist after update</b>	<p>When selected, counters that no longer exist after the monitor periodically scans the cluster manager and it's connected Docker nodes, are still displayed in the monitor (they are displayed as unavailable). Counters might no longer exist when a Docker node is disconnected from the cluster in which it is monitored, or the container is removed from the Docker node.</p> <p>This is useful, for example, for keeping track of counters that were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings on the next update.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> This option is relevant for dynamic counters only (those set using a regular expression). Static counters that are no longer available are still displayed even when this check box is cleared. For more details, see <a href="#">"Dynamic Docker Monitor Overview" on page 211</a>.</p>
<b>Enable secure connection</b>	<p>Enables SiteScope to connect to Docker REST APIs using a secure connection.</p> <p><b>Default value:</b> Not selected</p>
Proxy Settings	
<b>HTTP Proxy</b>	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the server.
<b>Proxy server user name</b>	<p>Proxy server user name if the proxy server requires a user name to access the server.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>

Main Settings	
UI Element	Description
<b>Proxy server password</b>	Proxy server password if the proxy server requires a user name to access the server. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy NTLM V2</b>	Select if the proxy requires authentication using NTLM version 2.
Authentication Settings	
<b>Credentials</b>	<p>Option to use for authorizing credentials if the Docker REST API specified requires a name and password for access:</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 Docker REST API 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 Docker REST API (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 How to Configure Credential Preferences in the Using SiteScope Guide.</li> </ul>
<b>Pre-emptive authorization</b>	<p>Option for sending authorization credentials if SiteScope requests the target Docker REST API:</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 Docker REST API. <b>Note:</b> If the Docker REST API does not require a user name and password, this option may cause the Docker REST API to fail.</li> <li>• <b>Authenticate if requested.</b> Select to send the user name and password on the second request if the Docker REST API requests a user name and password. <b>Note:</b> If the Docker REST API does not require a user name and password, this option may be used.</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>

Main Settings	
UI Element	Description
<b>Client side certificate</b>	<p>The certificate file, if you need to use a client side certificate to access the target Docker REST API. 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>	Password if you are using a client side certificate and that certificate requires a password.
<b>Authorization NTLM domain</b>	Domain for NT LAN Manager (NTLM) authorization if required to access the Docker REST API.
<b>Accept untrusted certificates for HTTPS</b>	If you are accessing a target server 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 <a href="#">"SSL Connectivity" on page 212</a> .
<b>Accept invalid certificates for HTTPS</b>	Select this option if you are accessing a target server 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.
<b>NTLM V2</b>	Select if the Docker REST API you are accessing requires authentication using NTLM version 2.
<b>Preferred protocols</b>	<p>Select the preferred protocol option to use for the handshake process.</p> <ul style="list-style-type: none"> <li>• <b>Any supported protocol.</b> Enables any supported protocol to be used for the handshake process (this is the default setting). Since this option uses SSL protocols, SSL must be enabled on the Web server to use this option.</li> <li>• <b>Prefer SSL to TLS.</b> Select if the server you are accessing cannot handle authentication using TLS. This enables encrypted handshake messages to be sent using SSL.</li> </ul> <p><b>Note:</b> This option is ignored (if selected) when SiteScope is running in FIPS 140-2 mode, since authentication using TLS is mandatory with FIPS 140-2. For details on FIPS 140-2, see the Running SiteScope Securely section of the SiteScope Deployment Guide (&lt;SiteScope root directory&gt;\sisdocs\doc_lib\Get_Documentation.htm).</p> <ul style="list-style-type: none"> <li>• <b>Prefer TLS to SSL.</b> Select if you prefer to use TLS for encrypting handshake messages or if the server you are accessing cannot handle authentication using SSL. TLS is the latest cryptographic protocol. TLS 1.0, 1.1, and 1.2 are supported.</li> </ul>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is a list of counters that can be configured when monitoring a cluster or a Docker node:

Cluster	Docker
<p><b>Cluster Counters</b></p> <ul style="list-style-type: none"> <li>• Daemon Counters <ul style="list-style-type: none"> <li>- Connect</li> </ul> </li> </ul> <p>Health Counters (for Cluster machine):</p> <ul style="list-style-type: none"> <li>• CPU <ul style="list-style-type: none"> <li>- Utilization</li> <li>- Utilization&lt;#&gt; (for each CPU)</li> </ul> </li> <li>• Disks <ul style="list-style-type: none"> <li>- Disk/File System percent full</li> <li>- Disk/File System MB free</li> <li>- Disk/File System MB total</li> </ul> </li> <li>• Memory <ul style="list-style-type: none"> <li>- MB free</li> <li>- physical memory MB free</li> <li>- physical memory MB used%</li> <li>- swap space MB free</li> <li>- swap space used%</li> </ul> </li> </ul> <p><b>Docker Counters</b></p> <p>All the counters in the Docker column for each Docker node in the cluster.</p>	<p><b>Docker Node Counters</b></p> <ul style="list-style-type: none"> <li>• List of Containers</li> <li>• Counters for all containers <ul style="list-style-type: none"> <li>- state</li> <li>- availability</li> </ul> </li> <li>• Counters for each running container: <ul style="list-style-type: none"> <li>- availability</li> <li>- cpu usage%</li> <li>- disk usage I/O read (bytes)</li> <li>- disk usage I/O read count</li> <li>- disk usage I/O write (bytes)</li> <li>- disk usage I/O write count</li> <li>- memory%</li> <li>- memory limit</li> <li>- memory usage</li> <li>- network usage received (bytes)</li> <li>- network usage transmitted (bytes)</li> <li>- state</li> </ul> </li> <li>• Daemon Counters (for each Docker node): <ul style="list-style-type: none"> <li>- Connect</li> <li>- Containers Amount</li> <li>- CPUs</li> <li>- Memory</li> </ul> </li> <li>• Health Counters for each Docker node (these counters are available only if there is a remote on the Docker node): <ul style="list-style-type: none"> <li>• CPU <ul style="list-style-type: none"> <li>- Utilization</li> <li>- Utilization&lt;#&gt; (for each CPU)</li> </ul> </li> <li>• Disks <ul style="list-style-type: none"> <li>- Disk/File System percent full</li> <li>- Disk/File System MB free</li> <li>- Disk/File System MB total</li> </ul> </li> <li>• Memory <ul style="list-style-type: none"> <li>- MB free</li> <li>- physical memory MB free</li> <li>- physical memory MB used%</li> <li>- swap space MB free</li> <li>- swap space used%</li> </ul> </li> </ul> </li> </ul>

## Tips/Troubleshooting

This section includes:

- ["General Notes/Limitations" below](#)
- ["Maximum Number of Counters That Can be Saved" below](#)
- ["Troubleshooting Dynamic Docker Monitor Logs" on the next page](#)
- ["Troubleshooting Dynamic Docker Application Discovery Logs" on the next page](#)

### General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When configuring the remote server name in the **Server** field of the UNIX Remote Server dialog box, you should use the same name that is configured in the Docker or cluster. For example, if the Docker uses an IP address to identify the server, then an IP address should be used in the remote server name. Failure to do this when monitoring a cluster results in the Docker nodes being displayed in a different hierarchy to the cluster when viewing the monitor in the Unified Console (**Hierarchy Monitors > Docker**).
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- You cannot move (cut and paste) a Dynamic Docker monitor if it has any dependencies, including auto discovered application monitor dependencies. Note that if you move an auto discovered application monitor, the link between the Dynamic Docker monitor and the application monitor is retained. If you make a copy of a Dynamic Docker monitor, any links between the copied Dynamic Docker monitor and the application monitors will be removed, and the discover mechanism will try to deploy a template on the monitored containers (of the copied monitor) as if it is a new monitor.
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).
- BSM Integration is partially supported; the monitor sends data and simple monitor CI topology to BSM. The monitor does not report the full Docker topology model to BSM.
- Operations Manager Integration is not supported. As a result, the monitor does not report events and metrics data to HPOM or OMi.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).

### Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the `_browsableContentMaxCounters` parameter in the `master.config` file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the `_maxCountersForRegexMatch` parameter in the `master.config` file. If during deployment,



the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The **\_maxCountersForRegexMatch** parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both **\_browsableContentMaxCounters** and **\_maxCountersForRegexMatch** parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

## Troubleshooting Dynamic Docker Monitor Logs

1. Check for dynamic framework errors in:

- **<SiteScope root directory>\logs\dynamic\_monitoring\_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
- **<SiteScope root directory>\logs\dynamic\_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).

To check for dynamic monitoring errors, copy the following section from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG in **<SiteScope root directory>\logs\docker\_monitor\docker\_monitor.log**.

```
#####  
# Dynamic Docker Monitor  
#####  
log4j.category.com.mercury.sitescope.monitors.facades.DynamicDockerMonitor=DEBUG, docker.appender  
log4j.additivity.com.mercury.sitescope.monitors.facades.DynamicDockerMonitor=false  
log4j.category.com.mercury.sitescope.monitors.docker.counterEntities=DEBUG, docker.appender  
log4j.additivity.com.mercury.sitescope.monitors.docker.counterEntities=false  
log4j.category.com.mercury.sitescope.monitors.docker.DockerSwarmInfo=DEBUG, docker.appender  
log4j.additivity.com.mercury.sitescope.monitors.docker.DockerSwarmInfo=false  
log4j.appender.docker.appender=org.apache.log4j.RollingFileAppender  
log4j.appender.docker.appender.File=../${log.file.docker_monitor.path}/docker_monitor.log  
log4j.appender.docker.appender.MaxFileSize=${def.file.max.size}  
log4j.appender.docker.appender.MaxBackupIndex=${def.files.backup.count}  
log4j.appender.docker.appender.layout=org.apache.log4j.PatternLayout  
log4j.appender.docker.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n  
log4j.appender.docker.appender.encoding=${general.encoding}
```

2. Check for Dynamic Docker monitor errors in:

- **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.

## Troubleshooting Dynamic Docker Application Discovery Logs

1. Check for Docker application discovery mechanism errors.

- To check for errors in the automatic Docker application discovery mechanism, copy the following section from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG in **<SiteScope root directory>\logs\docker\_monitor\app\_discover\_listener.log**,

**app\_discover\_scheduler.log, app\_discover\_config\_file\_updater.log, or app\_discover\_web\_ui\_requests.log.**

```
#####
# Dynamic Docker App Discover Appenders and loggers
#####
log4j.category.AppDiscoverListener=DEBUG, app_discover_listener.appender
log4j.additivity.AppDiscoverListener=false

#
# app_discover_listener appender
#

log4j.appender.app_discover_listener.appender=org.apache.log4j.RollingFileAppender
log4j.appender.app_discover_listener.appender.File=./${log.file.docker_monitor.path}/app_
discover_listener.log
log4j.appender.app_discover_listener.appender.MaxFileSize=${def.file.max.size}
log4j.appender.app_discover_listener.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.app_discover_listener.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.app_discover_listener.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p -
%m%n
log4j.appender.app_discover_listener.appender.encoding=${general.encoding}

log4j.category.AppDiscoverScheduler=DEBUG, app_discover_scheduler.appender
log4j.additivity.AppDiscoverScheduler=false

#
# app_discover_scheduler appender
#

log4j.appender.app_discover_scheduler.appender=org.apache.log4j.RollingFileAppender
log4j.appender.app_discover_scheduler.appender.File=./${log.file.docker_monitor.path}/app_
discover_scheduler.log
log4j.appender.app_discover_scheduler.appender.MaxFileSize=${def.file.max.size}
log4j.appender.app_discover_scheduler.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.app_discover_scheduler.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.app_discover_scheduler.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p -
%m%n
log4j.appender.app_discover_scheduler.appender.encoding=${general.encoding}

log4j.category.AppDiscoverConfigFileUpdater=DEBUG, app_discover_config_file_updater.appender
log4j.additivity.AppDiscoverConfigFileUpdater=false

#
# app_discover_config_file_updater appender
#

log4j.appender.app_discover_config_file_updater.appender=org.apache.log4j.RollingFileAppender
log4j.appender.app_discover_config_file_updater.appender.File=./${log.file.docker_
monitor.path}/app_discover_config_file_updater.log
log4j.appender.app_discover_config_file_updater.appender.MaxFileSize=${def.file.max.size}
log4j.appender.app_discover_config_file_updater.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.app_discover_config_file_updater.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.app_discover_config_file_updater.appender.layout.ConversionPattern=%d [%t] (%F:%L)
%-5p - %m%n
log4j.appender.app_discover_config_file_updater.appender.encoding=${general.encoding}

#
# app_discover_web_ui_requests appender
#
```

```
log4j.appender.app_discover_web_ui_requests.appender=org.apache.log4j.RollingFileAppender
log4j.appender.app_discover_web_ui_requests.appender.File=../${log.file.docker_monitor.path}/app_
discover_web_ui_requests.log
log4j.appender.app_discover_web_ui_requests.appender.MaxFileSize=${def.file.max.size}
log4j.appender.app_discover_web_ui_requests.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.app_discover_web_ui_requests.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.app_discover_web_ui_requests.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-
5p - %m%n
log4j.appender.app_discover_web_ui_requests.appender.encoding=${general.encoding}
```

2. Check the following logs in the **<SiteScope root directory>\logs\docker\_monitor** folder:
  - **<SiteScope root directory>\logs\docker\_monitor\app\_discover\_listener.log**. This log contains information about:
    - i. Dynamic Docker monitor configuration changes, for example, if monitored containers are added to or deleted from the monitor, or if an existing container stops or is restarted.
    - ii. Dynamic Docker monitor deletion.
    - iii. Application group deletion.
  - **<SiteScope root directory>\logs\docker\_monitor\app\_discover\_scheduler.log**. This log contains information about all of the discovery schedulers. For more details on the schedulers, see ["How to Configure the Automatic Discovery Mechanism Schedulers" on page 221](#).
  - **<SiteScope root directory>\logs\docker\_monitor\app\_discover\_config\_file\_updater.log**. This log contains information about new and updated config files. Check this file to ensure that the configuration loaded properly. This is dependent on the frequency that the config file is checked for changes, which is determined by the **dynamicDockerAppDiscoverConfigFilesSampleRateInSeconds** property in the **SiteScope root\groups\master.config** file. For details, see the ["How to Configure the Automatic Discovery Mechanism Schedulers" on page 221](#).
  - **<SiteScope root directory>\logs\docker\_monitor\app\_discover\_web\_ui\_requests.log**. This log contains information about requests to the applications discovered from the Unified Console (Web user interface).

# Chapter 29: Dynamic JMX Monitor

The Dynamic JMX monitor enables you to monitor performance statistics of those Java-based applications that provide access to their statistics by using the standard JMX remoting technology defined by JSR 160 (remote JMX). It enables you to select the same measurements that are available on a JMX monitor, or use the dynamic monitoring mechanism that recognizes changes on the monitored Java applications to automatically update the MBean counters and thresholds as they change during runtime.

You can create one JMX monitor instance for each application you are monitoring, or several monitors for the same application that analyze different counters.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Dynamic JMX monitor.

## Learn About

This section includes:

- ["Dynamic JMX Monitor Overview" below](#)
- ["Supported Platforms/Versions" on the next page](#)
- ["Applications Supporting JSR 160" on the next page](#)
- ["WebLogic Application Server Topology" on page 238](#)
- ["Connection Pool Settings" on page 239](#)
- ["Thread Pool Settings" on page 240](#)
- ["License Consumption" on page 241](#)

## Dynamic JMX Monitor Overview

This monitor enables you to:

- **Use static counters.** Monitor specific counters on a JMX application using static counters. 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.
- **Use dynamic monitoring.** Select the counter patterns you want to monitor using a regular expression or a static string, and let the monitor dynamically update MBean counters that match the pattern defined by the regular expression. Dynamic monitoring enables you to configure the monitor on a one time basis, and leave it to update itself.

When configuring a dynamic monitor, you can define a counter pattern that specifies the MBean counters you want to monitor. The monitor scans the target host periodically, and creates the counters that are aligned with the given counter pattern.

If a new MBean is added to the machine and part or all of its counters correspond to the counter pattern, the counters that match the counter pattern are automatically added to the monitor when the counters are next updated from the server. Similarly, if an MBean that corresponds to the counter pattern is no longer

available, counters for that MBean are removed from the monitor (unless you choose not to delete them, in which case they are still displayed in the monitor's counter list).

You can also define the required thresholds for the counter's pattern. In this way, thresholds are also updated automatically when the counters are updated.

For more details on the dynamic monitoring mechanism, see Dynamic Monitoring Mechanism in the Using SiteScope Guide.

**Note:**

- When monitoring a WebLogic Application Server using a t3 or t3s protocol, you need to use WebLogic's own protocol provider package. For details, see ["How to monitor a WebLogic 11g \(10.3.1-10.3.5\) or 12c server with an SSL connection using the t3, t3s, iiop or iiops protocol" on page 244.](#)
- SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of a WebLogic Application server. For details, see WebLogic Solution Templates in the Using SiteScope Guide.

## Supported Platforms/Versions

This monitor supports monitoring on:

- WebLogic 11g (10.3.1-10.3.5), 12c
- Apache Tomcat 5.0, 5.5, 6.0, 6.0.33, 7.0.25, 7.0.50, 7.0.61, 7.0.62, 8.0.23
- Oracle Application Server 10.1.3g
- JBoss servers 4.0.3, 4.2, 5.0, 5.1, 6.0, 6.1, 7.0, 7.1.x
- JBoss EAP 6.1.x - 6.2.x, 6.3.0
- Sun Glassfish Enterprise Server 2.1, 3.1
- WildFly 8.0.0, 8.1.0, 8.2.0

## Applications Supporting JSR 160

Here are some applications that currently support JSR 160 and information about how to monitor them:

- Oracle WebLogic 11g (10.3.1-10.3.5) and 12c support JSR 160, which can be enabled on the WebLogic application server by following instructions found on the [Oracle Web site](http://download.oracle.com/docs/cd/E14571_01/apirefs.1111/e13952/taskhelp/channels/EnableAndConfigureIIOP.html) ([http://download.oracle.com/docs/cd/E14571\\_01/apirefs.1111/e13952/taskhelp/channels/EnableAndConfigureIIOP.html](http://download.oracle.com/docs/cd/E14571_01/apirefs.1111/e13952/taskhelp/channels/EnableAndConfigureIIOP.html)).

Once enabled, the JMX URL for monitoring the server follows the following form:

```
service:jmx:iiop://<host>:<port>//jndi/weblogic.management.mbeanservers.  
runtime
```

or

```
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.

- Tomcat 5.x and 6.0 support 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 [Oracle Web site](http://download.oracle.com/javase/1.5.0/docs/guide/jmx/tutorial/security.html) for more details (<http://download.oracle.com/javase/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.

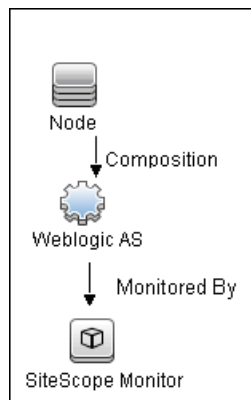
- JBoss 4.0.3 supports JSR 160, by defining the following properties to the JVM on startup:
  - `-Dcom.sun.management.jmxremote`
  - `-Dcom.sun.management.jmxremote.port=9999`
  - `-Dcom.sun.management.jmxremote.ssl=false`
  - `-Dcom.sun.management.jmxremote.authenticate=false`
  - `-Djboss.platform.mbeanserver`
  - `-Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServerBuilderImpl`
- JBoss 6.1 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.authenticate=false`
  - `-Dcom.sun.management.jmxremote.ssl=false`
  - `-Djboss.platform.mbeanserver`
  - `-Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServerBuilderImpl`
  - `-Djava.endorsed.dirs="%JBOSS_ENDORSED_DIRS%"`
  - `-classpath "%JBOSS_CLASSPATH%" org.jboss.Main %*`
- 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) (<http://www.jcp.org/en/jsr/detail?id=160>).

## WebLogic Application Server Topology

The Dynamic JMX monitor can identify the topology of WebLogic Application Servers. If **Report monitor**

**and related CI topology** is selected in **HP Integration Settings** (the default setting), the monitor creates the following topology in BSM's RTSM.



**Note:** By default, the Dynamic JMX monitor reports topology data to BSM when monitoring the WebLogic application server only. To report topology data when monitoring any other environment (such as JBoss or Oracle), you need to type the server name and hostname into the CI type key attributes fields in **HP Integration Settings > Topology Settings**.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

## Connection Pool Settings

The Dynamic JMX monitor uses connection pools to reduce the load on the JMX infrastructure and SiteScope. Connection pools provide reusable connections by the monitor itself during different monitor runs, and by several monitors that use the same connection details.

The connection pool is a set of pools per key. A key is the combination of a JMX URL, a user, and a password. If all JMX monitors are configured with the same JMX URL, user, and password, one connection pool is created. For two JMX applications and two different users, four connection pools are created.

The connection pool evicts idle connections according to the maximum number of idle connections allowed (configurable in **Dynamic JMX connection pool: maximum idle connections in pool (per key)**). Connections are evicted based on evictable idle time (configurable in **Dynamic JMX connection pool: minimum evictable idle time (milliseconds)**) and running the eviction thread (configurable in **Dynamic JMX connection pool: time between eviction runs (milliseconds)**).

### Process for Requesting a Connection from the Pool

1. If the connection pool key does not exist yet, a new pool is created for this key.
2. If the pool exists and there is an idle connection, the connection is returned.
3. If there is not an idle connection, a new connection is created until the maximum number of active connections in the pool is reached (**Dynamic JMX connection pool: maximum active connections in pool (per key)**), or until the maximum total connections in the pool is reached (**Dynamic JMX connection pool: total number of connections for whole pool**).
4. When the maximum number of active connections in the pool (per key) or maximum total connections is reached, the monitor waits x milliseconds (**Dynamic JMX connection pool: waiting for connection timeout (milliseconds)**) for a connection to be freed.
5. If one of the connections is freed in the meantime, it will be returned. Otherwise, the connection fails.

You can tune the following connection pool properties in **Preferences > Infrastructure Preferences > Monitor Settings**, as required:

- **Dynamic JMX connection pool: minimum evictable idle time (milliseconds):** The minimum time that a connection must be idle before the eviction thread can evict it. Note that the actual amount of time a connection will be idle depends on when the eviction thread runs (Dynamic JMX connection pool: time between eviction runs (milliseconds)). The default value is 1800000 milliseconds (30 minutes).
- **Dynamic JMX connection pool: time between eviction runs (milliseconds):** Interval between eviction thread runs for closing idle connections. The default value is 600000 milliseconds (10 minutes).
- **Dynamic JMX connection pool: maximum active connections in pool (per key):** The maximum number of active connections that can be open in the connection pool at the same time per key. (The connection pool is a set of pools per key. A key is the combination of a JMX URL, a user, and a password). The default value is 10.
- **Dynamic JMX connection pool: maximum idle connections in pool (per key):** The maximum number of idle connections in the connection pool (per key). (The connection pool is a set of pools per key. A key is the combination of a JMX URL, a user, and a password). When this value is exceeded, the number of unused connections that exceed this value are closed rather than kept in the connection pool. The default value is 5.
- **Dynamic JMX connection pool: total number of connections for whole pool:** The total number of dynamic JMX connections available for the JMX connection pool (for all the keys together). When this number is exceeded, the number of connections that exceed this value are closed. The default value is 500.
- **Dynamic JMX connection pool: waiting for connection timeout (milliseconds):** The amount of time to wait for a connection from the JMX connection pool before timing out. The default value is 60000 milliseconds (1 minute).

## Thread Pool Settings

The Dynamic JMX monitor always uses a separate thread pool to bring information (counter names and values) from the JMX server, unlike the JMX monitor which has two modes for using thread pools: regular mode and sandbox mode.

You can configure JMX thread pool settings in **Preferences > Infrastructure Preferences > Monitor Settings**. These settings are for each thread pool. A new thread pool is created for each additional classpath used by the Dynamic JMX monitor. The same thread pool is used for all Dynamic JMX monitors that do not use an additional classpath. Additional classpath is used if your MBean classes are not part of SiteScope classpath.

- **JMX thread pool core size:** Number of threads to keep in the JMX pool that can be created for JMX tasks, even if they are idle. The default value is 10.
- **JMX thread pool idle time (seconds):** When the number of threads is greater than the core, this is the maximum time that excess idle threads will wait for new JMX tasks before timing out. The default value is 30 seconds.
- **JMX thread pool maximum size:** Maximum number of threads to allow in the pool. If the number of threads in the pool is greater than the core but less than the maximum and the queue is full, then new threads will be created for the JMX tasks until the maximum number of threads in pool is reached. The default value is 200.
- **JMX thread pool queue size:** Maximum number of JMX tasks that can be added to the queue. If all the core threads are busy now, the new tasks will be added to queue until the max queue size is reached. The default value is 400.



## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitored object. An object is a path in the tree (not containing the counter name itself) for which at least one direct counter is selected.	One OSi license per monitored host

## Tasks

This section includes the following tasks:

- "How to Configure the Dynamic JMX Monitor" below
- "How to create a Dynamic JMX Monitor for JBoss 7.1, JBoss EAP 6.1.x - 6.2.x, or WildFly 8.0.0" on page 243
- "How to monitor a WebLogic 11g (10.3.1-10.3.5) or 12c server with an SSL connection using the t3, t3s, iiop or iiops protocol" on page 244

## How to Configure the Dynamic JMX Monitor

### 1. Configure the monitor properties

- a. Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **Dynamic JMX**. The New Dynamic JMX Monitor dialog box opens.
- b. In the General Settings panel, enter a name and description for the monitor.
- c. In the Dynamic JMX Monitor Settings panel, enter the required settings as described in "Dynamic JMX Monitor Settings" on page 246.

- For a WebLogic 11g (10.3.1-10.3.5) or 12c server, enter the following when configuring the monitor:

- In the **JMX URL** box, enter:

```
service:jmx:iiop://<host>:<port>//jndi/weblogic.management.  
mbeanservers.runtime
```

or


```
service:jmx:iiop:///jndi/iiop://<host>:<port>/weblogic.  
management.mbeanservers.runtime
```

- In the **Additional Classpath** box, enter the **wlfullclient.jar**.

You can specify the timeout for JMX task execution (mbeans retrieval and conversion into xml) by modifying the `_overallJMXCountersRetrievalTimeout` property in the `master.config` file. The default value is 15 minutes. This is not an ORB timeout.

**Note:** For details on creating the **wlfullclient.jar**, refer to the Oracle documentation on Using the WebLogic JarBuilder Tool ([http://download.oracle.com/docs/cd/E12840\\_01/wls/docs103/client/jarbuilder.html](http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html)).

- For monitoring WebLogic 11g or 12c using a t3 or t3s protocol: You need to use WebLogic's own protocol provider package as described in "How to monitor a WebLogic 11g (10.3.1-10.3.5) or 12c server with an SSL connection using the t3, t3s, iiop or iiops protocol" on page 244.

- For a WebLogic 6.x, 7.x, and 8.x server: To help you to select the counters that you require, you can open a WebLogic monitor for versions prior to WebLogic 9.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.
- d. In the **Patterns & Counter** section, click the **Get Counter** button, and select the counters you want to monitor from the Select Counters Form (the form displays static counters only). The counters are added to the Counter Preview tree.
- e. For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
  - Clicking the **Add New Counter**  button to add an empty line to the table, and then by creating a pattern format using a regular expression.

**Tip:**

- The pattern should always start and end with the forward slash ("/") character.
- The "[" and "]" characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character)
- Use "." to describe any character any number of times.


For example, `/java.lang/Memory/.*/` shows all memory counters that are exposed by the `java.lang` domain.

- Selecting a static counter, and editing the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.

**Note:** For details on the maximum number of counters that can be selected from the browsable tree and the maximum number of counters that can match the selected counter patterns when creating and updating dynamic monitors, see Troubleshooting and Limitations. If the maximum number of counters that can be deployed is exceeded, an error is written to the **RunMonitor.log**.

**Example:**

If you enter the pattern `/java.lang/ClassLoading/.*/`, the monitor retrieves all the `ClassLoading` counters in the JMX application, such as `TotalLoadedClassCount`, `UnloadedClassCount`, `LoadedClassCount`, `ObjectName`.

- f. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counter Preview tree.
- g. Set the frequency for updating counters from the server in the **Frequency of updating counters from server** box. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- h. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful for keeping track of the counters that were previously being monitored.
- i. Click **Verify & Save** or **Save** to save your settings.

- j. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

**Note:** When configuring threshold settings for the Dynamic JMX monitor:

- The monitor **always(default)** counter configured in the **Good if** section of the monitor's properties means that the state of the monitor is good, unless one of the thresholds of any of the other counters is breached.
- The **countersinError** counter configured in the **Error if** section of the monitor's properties means that the state of the monitor is error if one of the other counters is unavailable.

## 2. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["WebLogic Application Server Topology" on page 238](#).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

## 3. Configure connection pool and thread pool settings - optional

You can tune the connection pool and thread pool properties in **Preferences > Infrastructure Preferences > Monitor Settings**.

For details, see ["Connection Pool Settings" on page 239](#) and ["Thread Pool Settings" on page 240](#).

## 4. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the server where the JMX performance counters you want to monitor are running and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:

- The SiteScope **Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

## How to create a Dynamic JMX Monitor for JBoss 7.1, JBoss EAP 6.1.x - 6.2.x, or WildFly 8.0.0

Configure the monitor properties as described in the UI Descriptions section below.

**Note:** To get counters from a JBoss 7.1.x, JBoss EAP 6.1.x - 6.2.x, or WildFly 8.0.0 server, you must:

1. Add the following jars to classpath:
  - **jboss-common-core.jar**

- **jboss-client.jar**

2. Select the **Load additional classpath first** check box.

## How to monitor a WebLogic 11g (10.3.1-10.3.5) or 12c server with an SSL connection using the t3, t3s, iiop or iiops protocol

When monitoring a WebLogic Application Server using a t3, t3s, iiop or iiops protocol, you need to use WebLogic's own protocol provider package.

### Note:

- This task is part of a higher-level task. For details, see ["How to Configure the Dynamic JMX Monitor" on page 241](#).
- When monitoring a WebLogic server with the Administration port enabled, the t3s protocol must be used.

1. Enter the URL in the following format in the **JMX URL** box of JMX Monitor Settings:

- **For t3 protocol:**

```
service:jmx:t3://<host>:<port>/jndi/weblogic.management.  
mbeanservers.runtime
```

where the default port for t3 protocol is 7001

- **For t3s protocol:**

```
service:jmx:t3s://<host>:<port>/jndi/weblogic.management.  
mbeanservers.runtime
```

where the default port for t3s protocol is 7002

- **For iiop protocol:**

```
service:jmx:iiop://<host>:<port>/jndi/weblogic.management.mbeanservers.  
runtime
```

or

```
service:jmx:iiop:///jndi/iiop://<host>:<port>/weblogic.management.  
mbeanservers.runtime
```

- **For iiops protocol:**

```
service:jmx:iiops://host:port/jndi/weblogic.management.  
mbeanservers.runtime
```

2. (For t3 or t3s protocols) Copy the following jars from the WebLogic library to any folder on the SiteScope server:

- **%WEBLOGIC\_HOME%\server\lib\wlclient.jar**
- **%WEBLOGIC\_HOME%\server\lib\wljmxclient.jar**
- **%WEBLOGIC\_HOME%\server\lib\weblogic.jar**
- **%WEBLOGIC\_HOME%\server\lib\wlfullclient.jar**

- **%WEBLOGIC\_HOME%\server\lib\webserviceclient+ssl.jar** (for t3s protocol only)
- **%WEBLOGIC\_HOME%\server\lib\cryptoj.jar** (for t3s protocol only, if this file is present in WebLogic library)

Specify the full path to the copied jars in the **Additional Classpath** field in the JMX Monitor Settings separated by “,”.

**Note:** For details on creating the **wlfullclient.jar**, refer to the Oracle documentation on Using the WebLogic JarBuilder Tool ([http://download.oracle.com/docs/cd/E12840\\_01/wls/docs103/client/jarbuilder.html](http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html)).

3. (For iiop or iiops protocols) Copy the following jars from the WebLogic library to any folder on the SiteScope server:

- **%WEBLOGIC\_HOME%\server\lib\wlfullclient.jar**
- **%WEBLOGIC\_HOME%\server\lib\wlcipher.jar** (for iiops protocol only)

Specify the full path to **wlfullclient.jar** in the **Additional Classpath** field in the JMX Monitor Settings.

For details on creating the **wlfullclient.jar**, refer to the Oracle documentation on Using the WebLogic JarBuilder Tool ([http://download.oracle.com/docs/cd/E12840\\_01/wls/docs103/client/jarbuilder.html](http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html)).




4. (For t3s and iiops protocols) Enable SSL on the WebLogic server and import the SSL certificate into the SiteScope keystore. For details, see Certificate Management Overview.
5. Configure the other monitor settings as required.  
For details, see Common Monitor Settings in the Using SiteScope Guide.

# UI Descriptions

## Dynamic JMX Monitor Settings

User interface elements are described below:

UI Element	Description
<b>JMX URL</b>	<p>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></p> <ul style="list-style-type: none"><li>When creating a JMX monitor for a WebLogic 11g or 12c server, enter the following URL: <code>service:jmx:iiop://&lt;host&gt;:&lt;port&gt;///jndi/weblogic.management.mbeanservers.runtime</code> or <code>service:jmx:iiop:///jndi/iiop://&lt;host&gt;:&lt;port&gt;/weblogic.management.mbeanservers.runtime</code></li><li>When creating a JMX monitor for a JBoss server, your system administrator should configure the JBoss server, and then report which ports are enabled for JMX access.</li><li>When creating a JMX monitor for a JBoss 7.1 or JBoss EAP 6.1.x - 6.2.x server, enter the following URL: <code>service:jmx:remoting-jmx://&lt;host&gt;:&lt;port&gt;</code></li><li>When creating a JMX monitor for a WildFly 8.0.0 server, enter the following URL: <code>service:jmx:http-remoting-jmx://&lt;host&gt;:&lt;port&gt;</code></li><li>If you are using a t3 or t3s protocol, you need to use WebLogic's own protocol provider package and the JMX URL is in a different format. For details, see <a href="#">"How to monitor a WebLogic 11g (10.3.1-10.3.5) or 12c server with an SSL connection using the t3, t3s, iiop or iiops protocol"</a> on page 244.</li><li>The JMX over RMI protocol is not firewall friendly.</li></ul>
<b>Domain filter</b>	<p>Domain filter to show only those counters existing within a specific domain (optional). This filter does not have full regular expression support.</p> <p>You can specify the domain name or full path to MBean. The full path can be taken from the MBean <code>objectName</code> property using JConsole.</p> <p><b>Example:</b> Note that these MBean examples have different node properties in the path: <code>type-host-path</code> in the first and <code>type-resource-type-name</code> in the second.</p> <ul style="list-style-type: none"><li>For MBean "Catalina/Cache/localhost/SiteScope" specify: <code>"Catalina:type=Cache,host=localhost,path=/SiteScope"</code></li><li>For MBean "Catalina/Environment/Global/simpleValue" specify: <code>"Catalina:type=Environment,resourceType=Global,name=simpleValue"</code></li></ul>

UI Element	Description
<b>User name</b>	User name for connection to the JMX application (if required by your JMX application).
<b>Password</b>	Password for connection to the JMX application (if required by your JMX application).
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, to wait for a response from the server before timing-out. After this time period passes, the monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 60 seconds (using a value other than the default timeout value may adversely affect performance)</p>
<b>Additional classpath</b>	<p>The classpath library that is used to resolve unknown classes retrieved from the JMX server. Use additional classpath if your MBean classes are not part of SiteScope classpath. Multiple libraries can be entered separated by a semicolon.</p> <p>The Dynamic JMX monitor always uses a separate thread pool to bring information (counter names and values) from the JMX server, unlike the JMX monitor which has two modes for using thread pools: regular mode and sandbox mode. For details, see "<a href="#">Thread Pool Settings</a>" on page 240.</p> <p><b>Note:</b> When monitoring a WebLogic Application Server 11g (10.3.1 - 10.3.5) or 12c, this field is mandatory, and the <b>wlfullclient.jar</b> must be used. For details on creating the <b>wlfullclient.jar</b>, refer to Using the WebLogic JarBuilder Tool (<a href="http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html">http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html</a>).</p>
<b>Load additional classpath first</b>	Loads the additional classpath libraries before loading all the existing classpath libraries. If no additional classpath libraries are found, the other classpaths folders are loaded.
<b>Patterns &amp; Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Click the <b>Add New Counter</b>  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the <b>Delete Counter</b>  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the <b>View Matches for Selected Pattern Counter</b>  button to display counters that match the selected patterns.</p> <p><b>Note:</b> SiteScope uses Perl regular expressions for pattern matching. For example, if you enter <code>/cpu.*</code> or <code>cpu</code>, any counters with <code>cpu</code> in their name match this pattern and are added to the counters list.</p>
<b>Get Counters</b>	<p>Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.</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>

UI Element	Description
<b>Counter Preview</b>	Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.
<b>Frequency of updating counters from server</b>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p><b>Default value:</b> 1 hour</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The update frequency cannot be less than the monitor run frequency in Monitor Run Settings.</li> <li>• When configuring this setting in a template, the variable value can only be in time units of seconds.</li> <li>• Static counters are never deleted.</li> </ul>
<b>Continue displaying counters that no longer exist after update</b>	<p>When selected, counters that no longer exist after running the update mechanism to retrieve counters from the monitored server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful, for example, if a disk fails or for keeping track of counters that were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings on the next update.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> This option is relevant for dynamic counters only (those set using a regular expression). Static counters that are no longer available are still displayed even when this check box is cleared.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes

- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).



## Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the **\_browsableContentMaxCounters** parameter in the **master.config** file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the **\_maxCountersForRegexMatch** parameter in the **master.config** file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The **\_maxCountersForRegexMatch** parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both **\_browsableContentMaxCounters** and **\_maxCountersForRegexMatch** parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

## Troubleshooting Logs

1. Check for dynamic framework errors in:

- **<SiteScope root directory>\logs\dynamic\_monitoring\_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
- **<SiteScope root directory>\logs\dynamic\_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).

To check for dynamic monitoring errors, copy the following section from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####  
# Dynamic Monitoring  
#####  
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=  
DEBUG, dynamic.monitoring.appender  
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=false  
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG, dynamic.monitoring.appender  
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false  
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFileAppender  
log4j.appender.dynamic.monitoring.appender.File=./${log.file.path}/dynamic_monitoring.log  
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB  
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5  
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.PatternLayout  
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
```

2. Check for Dynamic JMX monitor errors in:

- **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.

- **<SiteScope root directory>\logs\dynamic\_monitoring.log\dynamic\_jmx\_monitor.log**. This log provides information about Dynamic JMX monitor errors.

To view JMX monitor errors, copy the following sections from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####  
Dynamic JMX monitor  
#####  
log4j.category.com.mercury.sitescope.monitors.facades.DynamicJMXMonitor=DEBUG,  
dynamicjmx.appender  
log4j.additivity.com.mercury.sitescope.monitors.facades.DynamicJMXMonitor=false  
log4j.category.com.mercury.sitescope.monitors.jmx=DEBUG, dynamicjmx.appender  
log4j.additivity.com.mercury.sitescope.monitors.jmx=false  
log4j.category.com.mercury.sitescope.infra.classpath=DEBUG, dynamicjmx.appender  
log4j.additivity.com.mercury.sitescope.infra.classpath=false  
  
log4j.appender.dynamicjmx.appender=org.apache.log4j.RollingFileAppender  
log4j.appender.dynamicjmx.appender.File=../${log.file.path}/dynamic_jmx_monitor.log  
log4j.appender.dynamicjmx.appender.MaxFileSize=${def.file.max.size}  
log4j.appender.dynamicjmx.appender.MaxBackupIndex=${def.files.backup.count}  
log4j.appender.dynamicjmx.appender.layout=org.apache.log4j.PatternLayout  
log4j.appender.dynamicjmx.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n  
log4j.appender.dynamicjmx.appender.encoding=${general.encoding}
```

# Chapter 30: e-Business Transaction Monitor

The e-Business Transaction monitor enables you to verify that the multiple tasks that make up an online transaction are completed properly.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the e-Business Transaction monitor.

## Learn About

This section includes:

- ["e-Business Transaction Monitor Overview" below](#)
- ["Editing the Order of the Monitors in the Chain" on the next page](#)
- ["License Consumption" on the next page](#)

### e-Business Transaction Monitor Overview

Use this monitor to verify that an end-to-end transaction and associated processes complete properly. This includes:

- Successful navigation through a series of URLs.
- Transmission of an email confirming the sequence.
- Logging the information into a database file.

The e-Business Transaction monitor runs a sequence of other SiteScope monitors, checking that each monitor returns a status of OK. It reports an Error status if any monitor in the sequence fails.

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 ["URL Sequence Monitor" on page 697](#)).
- Check that the order status was updated (see ["URL Sequence Monitor" on page 697](#)).
- Check that a confirmation email was received (see ["Mail Monitor" on page 362](#)).
- Check that the order was added to the order database (see ["Database Query Monitor" on page 169](#)).
- Check that the order was transferred to a legacy system (see ["Script Monitor" on page 580](#)).

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, groups, or both, currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

## 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.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	This is a free monitor that does not require any particular license type or available capacity.

# Tasks

## How to Configure the e-Business Transaction Monitor

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 (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).
- b. Open the new monitor group, and add the first individual monitor type needed for the sequence (for example, ["URL Sequence Monitor" on page 697](#)).

For task details on adding a monitor, see [How to Deploy a Monitor in the Using SiteScope Guide](#).

**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.

- 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. 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. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### e-Business Transaction Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>Monitor delay (seconds)</b>	<p>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>Error handling option during the sequence:</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>URL monitors 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>
<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 <a href="#">"Editing the Order of the Monitors in the Chain" on the previous page.</a></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> <p>For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page.</a></p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- % items OK
- % items in error
- % items in warning
- items OK
- items checked
- items in error
- items in warning
- name of the items in warning
- name of the items in error

## Tips/Troubleshooting

### General Tips/Limitations

This monitor cannot be copied to a template. It must be created directly in a template.

# Chapter 31: F5 Big-IP Monitor

This monitor enables you to monitor the content of event logs and other data from F5 Big-IP load balancing device using SNMP. 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. The error and warning thresholds for the monitor can be set on one or more load balancer statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the F5 Big-IP monitor.

## Learn About

### Supported Platforms/Versions

This monitor supports monitoring F5 Big-IP 4.0, 10.x, 11.x.

### IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSI license per monitored host

## Tasks

### How to Configure the F5 Big-IP Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Tip:** The **SNMP Browser Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Browser Tool in the Using SiteScope Guide.

# UI Descriptions

## F5 Big-IP Monitor Settings

User interface elements are described below:

UI Element	Description
<b>SNMP Settings</b>	
<b>Server</b>	Name of the server you want to monitor.
<b>Port</b>	Port to use when requesting data from the SNMP agent. <b>Default value:</b> 161
<b>F5 Big IP version</b>	Select the version of the monitored F5 Big IP system (4.x, 10.x, 11.x). <b>Default value:</b> 4.x



UI Element	Description
<b>MIB file</b>	<p>MIB file option:</p> <ul style="list-style-type: none"> <li>• <b>LOAD-BAL-SYSTEM-MIBS</b> file displays only those objects which are related to the 4.x version monitoring.</li> <li>• <b>F5-BIGIP-APM-MIB</b> file displays APM objects, such as access and connectivity statistics, pool statistics, and general APM information. Related to 10.x and 11.x versions monitoring.</li> <li>• <b>F5-BIGIP-COMMON-MIB</b> file displays common information for which all other BIG-IP MIB files reference, as well as the F5-specific SNMP traps. Related to 10.x and 11.x versions monitoring.</li> <li>• <b>F5-BIGIP-GLOBAL-MIB</b> file displays GTM objects, such as wide IPs, virtual servers, pools, links, servers, and datacenters. Related to 10.x and 11.x versions monitoring.</li> <li>• <b>F5-BIGIP-LOCAL-MIB</b> file displays LTM objects, such as virtual servers, pools, nodes, profiles, SNATs, health monitors, and iRules. Related to 10.x and 11.x versions monitoring.</li> <li>• <b>F5-BIGIP-SYSTEM-MIB</b> file displays BIG-IP system information, such as global statistic data, network information, and platform information. Related to 10.x and 11.x versions monitoring.</li> <li>• <b>F5-BIGIP-WAM-MIB</b> file displays WebAccelerator traffic objects, such as WebAccelerator specific statistic data, connection stats, or build information. Related to 10.x and 11.x versions monitoring.</li> <li>• <b>F5-BIGIP-EM-MIB</b> file displays Enterprise Manager objects, such as Device Lists, Device Groups and Images available on the system. Related to 11.x version monitoring.</li> <li>• <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. Related to 11.x version monitoring.</li> </ul> <p><b>Default value:</b> All MIBs</p>
<b>Counter calculation mode</b>	<p>Performs 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>

UI Element	Description
<b>Starting OID</b>	<p>Use 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>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> <p><b>Note:</b> This field is available in template mode only.</p>
<b>SNMP Connection Settings</b>	
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.</p> <p><b>Default value:</b> 5</p>
<b>Number of retries</b>	<p>Number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.</p> <p><b>Default value:</b> 1</p>
<b>Community</b>	<p>Community string (valid only for version 1 or 2 connections).</p> <p><b>Default value:</b> public</p>
<b>SNMP version</b>	<p>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 setting fields below.</p> <p><b>Default value:</b> V1</p>
<b>Authentication algorithm</b>	<p>The authentication algorithm to use for version 3 connections.</p> <p><b>Default value:</b> MD5</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>User name</b>	<p>User name for version 3 connections.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>Password</b>	<p>Authentication password to use for version 3 connections.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>Privacy algorithm</b>	<p>The privacy algorithm used for authentication for SNMP version 3 (DES, 128-Bit AES, 192-Bit AES, 256-Bit AES).</p> <p><b>Default value:</b> DES</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>Privacy password</b>	<p>Privacy password for version 3 connections. Leave blank if you do not want privacy.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>

UI Element	Description
<b>Context name</b>	Context Name to use for this connection. This is applicable for SNMP V3 only. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Context engine ID</b>	Hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>SNMP Counters</b>	
<b>Counters</b>	Displays 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>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a> .  <b>Note:</b> 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.  <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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<b>F5 systems</b> <ul style="list-style-type: none"> <li>• active</li> <li>• bitsin</li> <li>• bitsinHi32</li> <li>• bitsout</li> <li>• bitsoutHi32</li> <li>• concur • conmax</li> <li>• contot</li> <li>• cpuTemperature</li> <li>• droppedin</li> <li>• droppedout</li> <li>• fanSpeed</li> <li>• gatewayFailsafe</li> <li>• ifaddress</li> <li>• ifaddressTable</li> <li>• interface</li> <li>• loadbal</li> <li>• loadbalMode</li> <li>• loadBalTrap</li> <li>• member</li> <li>• memoryTotal</li> </ul>	<ul style="list-style-type: none"> <li>• memoryUsed</li> <li>• mirrorenabled</li> <li>• nat</li> <li>• ndaddr</li> <li>• nodePing</li> <li>• nodeTimeout</li> <li>• pktsin</li> <li>• pktsinHi32</li> <li>• pktsout</li> <li>• pktsouthHi32</li> <li>• pool</li> <li>• poolMember</li> <li>• portdeny</li> <li>• resetcounters</li> <li>• snat</li> <li>• snatConnLimit</li> <li>• snatTCPIidleTimeout</li> <li>• snatUDPIdleTimeout</li> <li>• sslProxy</li> <li>• sslProxyEntry</li> <li>• sslProxyTable</li> </ul>	<ul style="list-style-type: none"> <li>• unitId</li> <li>• uptime</li> <li>• vaddress</li> <li>• virtualAddress</li> <li>• virtualServer</li> <li>• vport</li> <li>• watchdogArmed</li> </ul> <b>F5 DNS</b> <ul style="list-style-type: none"> <li>• cache</li> <li>• dataCenters</li> <li>• globals</li> <li>• hosts</li> <li>• lbDnsSrvs</li> <li>• lbDomains</li> <li>• lbRouters</li> <li>• summary</li> </ul>
---	---	--

## Tips/Troubleshooting

### General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 32: File Monitor

The File monitor enables you to read a specified file and check the size and age of the file.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the File monitor.

## Learn About

This section includes:

- ["File Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Reading and Status" below](#)
- ["License Consumption" on the next page](#)

### 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 will 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.

### Supported Platforms/Versions

- This monitor supports monitoring UNIX remote servers that have been configured in SiteScope and the local SiteScope machine only.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop monitoring environment, see ["How to Configure the HP NonStop Resources Monitor" on page 307](#).

### 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.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor  Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

## Tasks

How to Configure the File Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Note:** The **Regular Expression Tool** is available when configuring this monitor. For details on the tool, see Regular Expression Tool in the Using SiteScope Guide.

## UI Descriptions

### File Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Server where the file you want to monitor is located. Select a server from the server list (only 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>

UI Element	Description
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 (if the monitor does not work for one of these conditions, the other condition must be fulfilled, since both conditions do not always work on some machines). For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>File name</b>	<p>Path and name to the file you want to monitor.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• It may be necessary to provide the full path to the target file. For example, <code>/opt/application/logs/user.log</code>.</li> <li>• 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 How to Configure SiteScope to Monitor a Remote UNIX Server in the Using SiteScope Guide.</li> <li>• For reading files on remote Windows servers, use NetBIOS to specify the server and UNC path to the remote log file. For example, <code>\\remoteserver\sharedfolder\filename.log</code>.</li> <li>• You can also monitor files local to the server where SiteScope is running. For example, <code>C:\application\appLogs\access.log</code>.</li> <li>• Optionally, you can use regular expressions for special date and time variables to match on 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 file. For details on using regular expressions and dates, see SiteScope Date Variables in the Using SiteScope Guide.</li> </ul>

UI Element	Description
<b>File encoding</b>	<p>File content is monitored using an encoding that is different than the encoding used on server where SiteScope is running. 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>
<b>Match content</b>	<p>Text string to match in the returned page or frameset. If the text is not contained in the page, the monitor displays the message content <code>match error</code>. The search is case sensitive.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>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. For example, <code>&lt; B&gt; Hello&lt; /B&gt; World</code>.</li> <li>You can also perform a regular expression match by enclosing the string in forward slashes, with a letter <code>i</code> after the trailing slash indicating case-insensitive matching. For example, <code>/href=Doc\d+\.html/</code> or <code>/href=doc\d+\.html/i</code>.</li> <li>You can search for a pattern string across multiple lines. To do so, add the <code>/s</code> modifier to the end of the regular expression. For example, <code>/(state).*(populate)/s</code> checks if the returned page contains both "state" and "populate".</li> <li>To save and display a particular piece of text as part of the status, use parentheses in a Perl regular expression. For example, <code>/Temperature: (\d+)</code> returns the temperature as it appears on the page, and this could be used when setting an Error if or Warning if threshold.</li> </ul> <p>For details on regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.</p>
<b>Open Tool</b>	<p>Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.</p>



UI 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, 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>The monitor remains in <b>Good</b> status even if the file is not found. The monitor status is Good regardless of how the monitor's thresholds have been configured.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- content match
- file age
- size
- status

# Chapter 33: Formula Composite Monitor

This monitor enables you to monitor 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Formula Composite monitor.

## Learn About

### 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.
- Microsoft Windows Performance Counter monitor.
- Script monitor.
- SNMP monitor.

If you need alert logic that is more complex than SiteScope's standard alerts permit, 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.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	Requires no additional licensing beyond the licensing requirements of the member monitors which it contains.

## Tasks

### How to Configure the Formula Composite Monitor

1. Prerequisites
  - You must create at least two individual Database Query, Microsoft Windows Performance Counter, Script, or SNMP monitor instances before you can set up a Formula Composite monitor for those

monitors. For details, see:

- ["Database Query Monitor" on page 169.](#)
- ["Microsoft Windows Performance Counter Monitor" on page 473.](#)

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.

- ["Script Monitor" on page 580.](#)
- ["SNMP Monitor" on page 615.](#)
- 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.

## 2. Configure the monitor properties



Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## Formula Composite Monitor Settings

User interface elements are described below:






UI 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. For details on the Add Items dialog box, see <a href="#">"Add Items Dialog Box" on the next page.</a></p> <p>To remove monitors from the list, select the monitors and the <b>Delete</b>  button.</p>
<b>Run monitors</b>	<p>The Formula Composite monitor controls 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>Counters</b>	<p>Server performance counters to check with this monitor. The list displays the available counters and those currently selected for this monitor.</p>

UI Element	Description
<b>Monitor delay (seconds)</b>	Amount of time, in seconds, to wait between running each monitor (if <b>Run monitors</b> is selected). <b>Default value:</b> 0 seconds
<b>Operation</b>	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.
<b>Constant</b>	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 <operator> <number>.  Valid operators are + (addition), - (subtraction), * (multiplication), and / (division). Numbers may be integers or decimals.
<b>Result label</b>	Name for the result of the formula calculation.

## Add Items Dialog Box

This dialog box enables you to select the monitors, groups, or both, that you want in the Composite monitor.

User interface elements are described below:

UI Element	Description
<b>Add Selected Items</b>	Click to add the selected groups, monitors, or both, to the Formula Composite monitor.
 SiteScope	Represents the SiteScope root directory.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors).  If a group alert has been set up for the monitor group or subgroup, the alert  symbol is displayed next to the group icon.
	Represents a SiteScope monitor (enabled/disabled).  If an alert has been set up for the monitor, the alert  symbol is displayed next to the monitor icon.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Tips/Limitations

- When copying this monitor to a template, the subordinate monitors used to build a Formula Composite monitor are not copied. Therefore, it is recommended to create this monitor and its subordinate monitors directly in a template.
- Use the Formula Composite monitor only 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.

# Chapter 34: FTP Monitor

This monitor enables you to log on to an FTP server and retrieve a specified file. A successful file retrieval indicates that your FTP server is functioning properly. The FTP monitor also supports secure FTP (SFTP).

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the FTP monitor.

## Learn About

This section includes:

- ["FTP Monitor Overview" below](#)
- ["Status" below](#)
- ["Scheduling the Monitor" on the next page](#)
- ["License Consumption" on the next page](#)

### 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 ensure the accessibility of FTP files. Each time the monitor runs (in FTP or SFTP mode), it opens a connection to the FTP server, downloads the specified file, and then closes the connection.

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.

### 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.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license for 10 monitors

# Tasks

## How to Configure the FTP Monitor

### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- Before you can use this monitor, make sure you know:
  - The relative paths, if any, to the files on the FTP server.
  - An applicable user name and password to access the files.
  - The filenames of one or more files available for FTP transfer.

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

#### Tip:

- The **FTP Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see FTP Tool in the Using SiteScope Guide.
- The FTP monitor matches text which it has downloaded to the content buffer. By default, the content buffer size is set to 50000 bytes. You can modify this value, if necessary, from

**Preferences > Infrastructure Preferences > Monitor Settings > FTP Content match maximum size.**

## UI Descriptions

### FTP Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Basic FTP Settings</b>	
<b>Protocol</b>	Select a protocol for the monitor: <ul style="list-style-type: none"><li>• <b>FTP</b>. The monitor supports non-secure sockets only.</li><li>• <b>SFTP</b>. The monitor supports Secure FTP. It typically uses SSH version 2 (TCP port 22) to provide secure file transfer. In this version, only password authentication is supported.</li></ul> <b>Note:</b> SFTP protocol does not support <b>Passive mode</b> and SFTP is encrypted, rendering traditional proxies ineffective for controlling SFTP traffic (the proxy fields are not available).
<b>FTP server</b>	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>	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 in the Using SiteScope Guide. <b>Example:</b> s/C:\\firstdir\\\$shortYear\$\$0month\$\$0day\$/
<b>User name</b>	Name used to log into the FTP server. A common user name for general FTP access is user name anonymous.
<b>Password</b>	Password used to log into the FTP server. If using the anonymous login, the password is also anonymous.
<b>Passive mode</b>	SiteScope uses FTP passive mode. You use this mode to enable FTP to work through firewalls. (Not available in SFTP mode.)
<b>Advanced FTP Settings</b>	



UI Element	Description
<b>Match content</b>	<p>Text string 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>
<b>Timeout (seconds)</b>	<p>Amount of time, in 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>File encoding</b>	<p>If the file content to be monitored uses an encoding that is different than the encoding used on the server where SiteScope is running, enter the 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>Default value:</b> windows-1252</p>
<b>Connection timeout (seconds)</b>	<p>Amount of time, in 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> (Not available in SFTP mode)	

UI Element	Description
<b>HTTP proxy</b>	SiteScope runs 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.  <b>Example:</b> proxy.thiscompany.com:8080  <b>Note:</b> The FTP monitor does not support an FTP Proxy server.
<b>Proxy user name</b>	Proxy user name if the proxy server requires a name and password to access the file. The proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy password</b>	Proxy password if the proxy server requires a name and password to access the file. The proxy server must support Proxy-Authenticate for these options to function.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- GET file transfer time
- GET file transfer rate
- PUT file transfer time
- PUT file transfer rate

# Chapter 35: Generic Hypervisor Monitor

The Generic Hypervisor monitor provides a solution for monitoring Virtual Machines by using the virsh tool (a command line interface tool for managing guests and the hypervisor) to collect detailed information on nodes and guest virtual machines running on the host. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch key operational factors that can seriously affect availability and degrade performance. Create a separate monitor instance for each server you are running.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Generic Hypervisor monitor.

## Learn About

This section includes:

- ["Generic Hypervisor Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["License Consumption" below](#)

### Generic Hypervisor Monitor Overview

SiteScope simplifies the monitoring of virtual infrastructure changes in dynamic, virtualized environments by automatically changing the SiteScope configuration according to changes in the virtual environment. Generic Hypervisor monitors are dynamically updated over time by adding or removing counters as virtual machines are added or removed. This enables you to configure the monitor one time, and leave it to automatically discover changes in the environment and update itself.

During initial monitor creation, the monitor uses the connection URI configured to access the VM 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.

You can also define the required thresholds for the counter's pattern. In this way, thresholds are also updated automatically when the counters are updated.

For details on the dynamic monitoring mechanism, see Dynamic Monitoring Mechanism in the Using SiteScope Guide.

### Supported Platforms/Versions

This monitor supports monitoring remote servers running on UNIX remotes only. It has been tested on a KVM environment.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per host and one point per guest	One OSi license per monitored host


# Tasks

## How to Configure the Generic Hypervisor Monitor

### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- The monitored VM server must be directly accessible by the SiteScope server (no proxy involved).
- The Virsh command-line tool should be installed on the system. For details, see <https://help.ubuntu.com/community/KVM/Virsh>.

### 2. Configure the monitor properties

- a. Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **Generic Hypervisor**. The New Generic Hypervisor Monitor dialog box opens.
- b. In the General Settings panel, enter a name and description for the monitor.
- c. In the Generic Hypervisor Monitor Settings panel, select the VM server you want to monitor (or add a new server) and specify the driver to which you want to connect in the **Connection URI** box. For user interface details, see the UI Descriptions section below.
- d. Click the **Get Counter** button, and select the counters you want to monitor from the Select Counters Form. The counters are added to the Preview tree in the **Patterns & Counters** section.
- e. For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
  - Clicking the **Add New Counter**  button to add an empty line to the table, and creating a pattern format using a regular expression.

#### Tip:

- (1). The pattern should always start and end with the forward slash ("/") character.
- (2). The "[" and "]" characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character).
- (3). Use "." to describe any character any number of times.


For example, `./*/Domains Information/./*/Used Memory/` displays Used Memory counter for all VMs.

- Selecting a static counter, and editing the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.

**Note:** For details on the maximum number of counters that can be selected from the browsable tree and the maximum number of counters that can match the selected counter patterns when creating and updating dynamic monitors, see ["Maximum Number of Counters That Can be Saved" on page 280](#). If the maximum number of counters that can be deployed is exceeded, an error is written to the **RunMonitor.log**.

**Example:**

If you enter the pattern `./*/Domains Information./*/Used Memory/`, the monitor retrieves the Used Memory counter for all VMs.

- f. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counter Preview tree.
- g. Set the frequency for updating counters from the server in the **Frequency of updating counters from server** box. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- h. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful for keeping track of the counters that were previously being monitored.
- i. Click **Verify & Save** or **Save** to save your settings.
- j. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

### 3. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the VM server and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:




- The **SiteScope Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

For additional troubleshooting suggestions, see ["Tips/Troubleshooting" on page 279](#).

# UI Descriptions

## Generic Hypervisor Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of the VM server that you want to monitor. Select a server from the server list (only those UNIX remote servers that have been configured in SiteScope are displayed), or click the <b>Add Remote Server</b> to add a new UNIX server.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>When configuring this monitor on SiteScopes running on UNIX versions, only remote servers that have been configured with an <b>SSH</b> connection method are displayed. For details, see How to Configure Remote Windows Servers for SSH monitoring.</li> <li>When working in template mode, 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> </ul>
<b>Add Remote Server</b>	<p>Opens the Add UNIX Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Connection URI</b>	<p>URI of the driver of the VM server that you want to monitor.</p>
<b>Patterns &amp; Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Click the <b>Add New Counter</b>  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the <b>Delete Counter</b>  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the <b>View Matches for Selected Pattern</b>  button to display counters that match the selected patterns.</p> <p><b>Note:</b> SiteScope uses Perl regular expressions for pattern matching.</p>
<b>Get Counters</b>	<p>Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.</p>
<b>Counter Preview</b>	<p>Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.</p>

UI Element	Description
<b>Frequency of updating counters from server</b>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p><b>Default value:</b> 15 minutes</p> <p><b>Note:</b></p> <ul style="list-style-type: none"><li>• The update frequency cannot be less than the monitor run frequency in Monitor Run Settings.</li><li>• When configuring this setting in a template, the variable value can only be in time units of seconds.</li><li>• Static counters are never deleted.</li></ul>
<b>Continue displaying counters that no longer exist after update</b>	<p>When selected, counters that no longer exist after running the update mechanism to retrieve counters from the monitored server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful, for example, if a disk fails or for keeping track of counters that were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings on the next update.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> This option is relevant for dynamic counters only (those set using a regular expression). Static counters that are no longer available are still displayed even when this check box is cleared.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section includes:

- ["General Notes" below](#)
- ["Maximum Number of Counters That Can be Saved" on the next page](#)
- ["Troubleshooting Logs" on the next page](#)

### General Notes

- When configuring this monitor in template mode, the **Add Remote Server** button is not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is

displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).

- This monitor supports setting fractional thresholds which are more useful than setting whole number thresholds when monitoring large disks (such as 1 terabyte and larger).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).

## Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the **\_browsableContentMaxCounters** parameter in the **master.config** file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the **\_maxCountersForRegexMatch** parameter in the **master.config** file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The **\_maxCountersForRegexMatch** parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both **\_browsableContentMaxCounters** and **\_maxCountersForRegexMatch** parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

## Troubleshooting Logs

1. Check for dynamic framework errors in:

- **<SiteScope root directory>\logs\dynamic\_monitoring\_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
- **<SiteScope root directory>\logs\dynamic\_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).

To check for dynamic monitoring errors, copy the following section from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####  
# Dynamic Monitoring  
#####  
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=  
DEBUG, dynamic.monitoring.appender  
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=false  
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG, dynamic.monitoring.appender  
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false  
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFileAppender  
log4j.appender.dynamic.monitoring.appender.File=../${log.file.path}/dynamic_monitoring.log  
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB  
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5
```



```
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.PatternLayout  
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
```

2. Check for Generic Hypervisor monitor errors in:
  - **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.

# Chapter 36: Hadoop Monitor

The Hadoop monitor enables you to dynamically monitor the health and performance statistics of Hadoop Distributed File System (HDFS) and Hadoop MapReduce master nodes of the Hadoop cluster infrastructure using the standard JMX remoting technology defined by JSR 160 (for details, see ["Applications Supporting JSR 160" on page 237](#)).

You can select measurements on specified Hadoop cluster hosts, or use the dynamic monitoring mechanism to automatically update counters and thresholds that changed during run-time.

You can create one monitor for each master node in your cluster, or several monitors to monitor the same master node that analyzes different counters.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of a Hadoop cluster. For details, see Hadoop Cluster Monitoring Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Hadoop monitor.

## Learn About

This section includes:

- ["Hadoop Monitor Overview" below](#)
- ["Supported Platforms/Versions" on the next page](#)
- ["Connection Pool Settings" on the next page](#)
- ["Thread Pool Settings" on page 284](#)
- ["Hadoop Topology" on page 284](#)
- ["License Consumption" on page 285](#)

## Hadoop Monitor Overview

This monitor enables you to:

- Monitor specific counters on a JMX application using static counters. 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.
- Select the counter patterns you want to monitor using a regular expression or a static string, and let the monitor dynamically update MBean counters that match the pattern defined by the regular expression. Dynamic monitoring enables you to configure the monitor on a one time basis, and leave it to update itself.

When configuring a dynamic monitor, you can define a counter pattern that specifies the MBean counters you want to monitor. You can also define the required thresholds for the counter's pattern. The monitor scans the target host periodically, and creates the counters that are aligned with the given counter pattern.

If a new MBean is added to the machine and part or all of its counters correspond to the counter pattern, the counters that match the counter pattern are automatically added to the monitor when the counters are

next updated from the server. Similarly, if an MBean that corresponds to the counter pattern is no longer available, counters for that MBean are removed from the monitor (unless you choose not to delete them, in which case they are still displayed in the monitor's counter list).

You can also select counter patterns to be used as threshold conditions. In this way, thresholds are also updated automatically when the counters are updated.

For more details on the dynamic monitoring mechanism, see *Dynamic Monitoring Mechanism* in the *Using SiteScope Guide*.

## Supported Platforms/Versions

This monitor supports monitoring Hadoop 1.x on GNU/Linux.

## Connection Pool Settings

The Hadoop monitor uses connection pools to reduce the load on the JMX infrastructure and SiteScope. Connection pools provide reusable connections by the monitor itself during different monitor runs, and by several monitors that use the same connection details.

The connection pool is a set of pools per key. A key is the combination of a JMX URL, a user, and a password. If all JMX monitors are configured with the same JMX URL, user, and password, one connection pool is created. For two JMX applications and two different users, four connection pools are created.

The connection pool evicts idle connections according to the maximum number of idle connections allowed (configurable in **Dynamic JMX connection pool: maximum idle connections in pool (per key)**). Connections are evicted based on evictable idle time (configurable in **Dynamic JMX connection pool: minimum evictable idle time (milliseconds)**) and running the eviction thread (configurable in **Dynamic JMX connection pool: time between eviction runs (milliseconds)**).

### Process for Requesting a Connection from the Pool

1. If the connection pool key does not exist yet, a new pool is created for this key.
2. If the pool exists and there is an idle connection, the connection is returned.
3. If there is not an idle connection, a new connection is created until the maximum number of active connections in the pool is reached (**Dynamic JMX connection pool: maximum active connections in pool (per key)**), or until the maximum total connections in the pool is reached (**Dynamic JMX connection pool: total number of connections for whole pool**).
4. When the maximum number of active connections in the pool (per key) or maximum total connections is reached, the monitor waits x milliseconds (**Dynamic JMX connection pool: waiting for connection timeout (milliseconds)**) for a connection to be freed.
5. If one of the connections is freed in the meantime, it will be returned. Otherwise, the connection fails.

You can tune the following connection pool properties in **Preferences > Infrastructure Preferences > Monitor Settings**, as required:

- **Dynamic JMX connection pool: minimum evictable idle time (milliseconds)**: The minimum time that a connection must be idle before the eviction thread can evict it. Note that the actual amount of time a connection will be idle depends on when the eviction thread runs (**Dynamic JMX connection pool: time between eviction runs (milliseconds)**). The default value is 1800000 milliseconds (30 minutes).
- **Dynamic JMX connection pool: time between eviction runs (milliseconds)**: Interval between eviction thread runs for closing idle connections. The default value is 600000 milliseconds (10 minutes).
- **Dynamic JMX connection pool: maximum active connections in pool (per key)**: The maximum number of active connections that can be open in the connection pool at the same time per key. (The

connection pool is a set of pools per key. A key is the combination of a JMX URL, a user, and a password). The default value is 10.

- **Dynamic JMX connection pool: maximum idle connections in pool (per key):** The maximum number of idle connections in the connection pool (per key). (The connection pool is a set of pools per key. A key is the combination of a JMX URL, a user, and a password). When this value is exceeded, the number of unused connections that exceed this value are closed rather than kept in the connection pool. The default value is 5.
- **Dynamic JMX connection pool: total number of connections for whole pool:** The total number of dynamic JMX connections available for the JMX connection pool (for all the keys together). When this number is exceeded, the number of connections that exceed this value are closed. The default value is 500.
- **Dynamic JMX connection pool: waiting for connection timeout (milliseconds):** The amount of time to wait for a connection from the JMX connection pool before timing out. The default value is 60000 milliseconds (1 minute).

## Thread Pool Settings

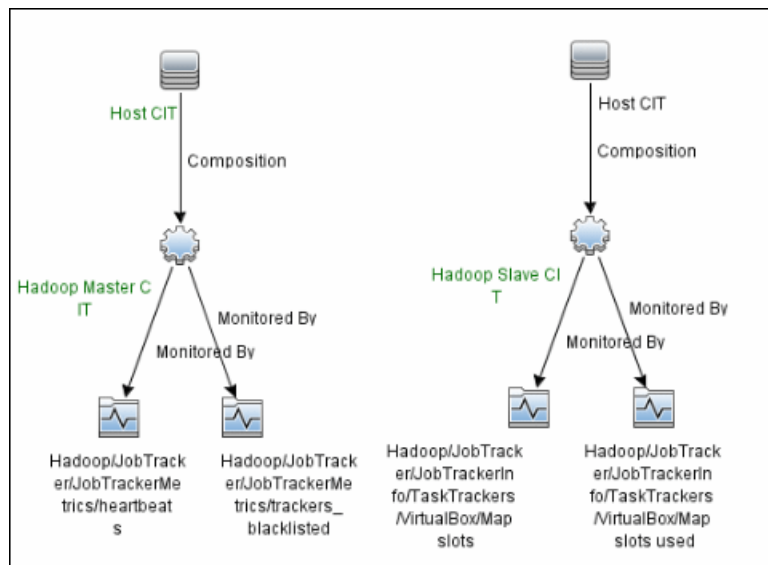
The Hadoop monitor always uses a separate thread pool to bring information (counter names and values) from the JMX server (unlike the JMX monitor which has two modes for using thread pools: regular mode and sandbox mode).

You can configure JMX thread pool settings in **Preferences > Infrastructure Preferences > Monitor Settings**. These settings are only relevant when using additional classpath mode. These settings are for each thread pool. A new thread pool is created for each additional classpath used by the Hadoop monitor. The same thread pool is used for all Hadoop monitors that do not use an additional classpath.

- **JMX thread pool core size:** Number of threads to keep in the JMX pool that can be created for JMX tasks, even if they are idle. The default value is 10.
- **JMX thread pool idle time (seconds):** When the number of threads is greater than the core, this is the maximum time that excess idle threads will wait for new JMX tasks before timing out. The default value is 30 seconds.
- **JMX thread pool maximum size:** Maximum number of threads allowed in the pool. If the number of threads in the pool is greater than the core but less than the maximum, and the queue is full, then new threads will be created for the JMX tasks until the maximum number of threads in pool is reached. The default value is 200.
- **JMX thread pool queue size:** Maximum number of JMX tasks that can be added to the queue. If all the core threads are busy now, the new tasks will be added to queue until the max queue size is reached. The default value is 400.

## Hadoop Topology

The Hadoop monitor can identify the topology of the Hadoop cluster infrastructure being monitored. If **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting), the monitor creates the following topology in BSM's RTSM.



For information about retrieving topologies and reporting them to BSM, see [Reporting Discovered Topologies to BSM in the Using SiteScope Guide](#).

**Note:**

- Topology reporting for this monitor is only supported in BSM 9.23 and later.
- The Hadoop monitor does not report the Hadoop Cluster CI type in the topology results. As a result, the default Hadoop cluster view does not show results reported by SiteScope.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitored object. An object is a path in the tree (not containing the counter name itself) for which at least one direct counter is selected).	One OSi license per monitored host


## Tasks

## How to Configure the Hadoop Monitor

## 1. Configure the monitor properties

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **Hadoop**. The New Hadoop Monitor dialog box opens.
- In the General Settings panel, enter a name and description for the monitor.
- In the Hadoop Monitor Settings panel, enter the required settings as described in "[Hadoop Monitor Settings](#)" on page 288.
- In the **Patterns & Counter** section, click the **Get Counter** button, and select the counters you want

to monitor from the Select Counters Form (the form displays static counters only). The counters are added to the Counter Preview tree.

- f. For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
  - Clicking the **Add New Counter**  button to add an empty line to the table, and then by creating a pattern format using a regular expression.

**Tip:**

- The pattern should always start and end with the forward slash ("/") character.
- The "[" and "]" characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character)
- Use ".\*" to describe any character any number of times.


For example, `/java.lang/Memory/.*/` shows all memory counters that are exposed by the `java.lang` domain.

- Selecting a static counter, and editing the counter to create a pattern format using a regular expression. For details on using regular expressions, see [Regular Expressions Overview](#) in the [Using SiteScope Guide](#).

**Note:** For details on the maximum number of counters that can be selected from the browsable tree and the maximum number of counters that can match the selected counter patterns when creating and updating dynamic monitors, see ["Tips/Troubleshooting" on page 293](#). If the maximum number of counters that can be deployed is exceeded, an error is written to the `RunMonitor.log`.

**Example:**

If you enter the pattern `/java.lang/ClassLoading/.*/`, the monitor retrieves all the `ClassLoading` counters in the JMX application, such as `TotalLoadedClassCount`, `UnloadedClassCount`, `LoadedClassCount`, `ObjectName`.

- g. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counter Preview tree.
- h. Set the frequency for updating counters from the server in the **Frequency of updating counters from server** box. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- i. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful for keeping track of the counters that were previously being monitored.
- j. Click **Verify & Save** or **Save** to save your settings.
- k. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see [Threshold Settings](#) in the [Using SiteScope Guide](#).

**Note:** When configuring threshold settings for the Hadoop monitor:

- The monitor **always(default)** counter configured in the **Good if** section of the monitor's properties means that the state of the monitor is good, unless one of the thresholds of any of the other counters is breached.
- The **countersinError** counter configured in the **Error if** section of the monitor's properties means that the state of the monitor is error if one of the other counters is unavailable.

## 2. Configure connection pool and thread pool settings - optional

You can tune the connection pool and thread pool properties in **Preferences > Infrastructure Preferences > Monitor Settings**.

For details, see "[Connection Pool Settings](#)" on page 283 and "[Thread Pool Settings](#)" on page 284.

## 3. Enable topology reporting - optional

- To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide. For details on the Hadoop monitor topology, see "[Hadoop Topology](#)" on page 284.
- To see topology reported by the monitor and Health Indicators assigned to monitor metrics, you should download and install the following resources from the HPE Live Network:

### Content Pack for DDM:

- i. Navigate to **HPE Live Network Home > Discovery and Dependency Mapping > Content Packs for DDM > Content Files** (<https://hpln.hp.com/node/31/contentfiles>).
- ii. In the resources tree, select: **Downloads > Content Packs for UCMDB 9.03 – 9.05 > DDM Content Pack 11 > Technology Specific Content**.
- iii. Download the **Hadoop** zip file and the installation instructions PDF.
- iv. Follow the instructions in the PDF for importing the content package into RTSM.

### Content Pack for BSM:

- i. Navigate to **HPE Live Network Home > Business Service Management > Content Packs for BSM > Content Files** (<https://hpln.hp.com/node/12361/contentfiles>).
- ii. In the resources tree, select: **Downloads > Content > Hadoop > 9.22**.
- iii. Download the zip file corresponding your BSM platform and the installation instructions PDF.
- iv. Follow the instructions in the PDF for installing the content pack.

## 4. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the server where the JMX performance counters you want to monitor are running and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:




- The SiteScope **Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.

- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

## UI Descriptions

### Hadoop Monitor Settings

User interface elements are described below:

UI Element	Description
<b>JMX URL</b>	<p>URL to gather JMX statistics. This is the hostname of the server which hosts the Hadoop Distributed File System (HDFS) and Hadoop MapReduce master nodes.</p> <p>Enter the URL in the format:</p> <pre>service:jmx:rmi:///jndi/rmi://&lt;host&gt;:&lt;port&gt;/jmxrmi</pre>
<b>Domain filter</b>	<p>Domain that is used to gather Hadoop statistics (optional). If this field is left blank, the default Hadoop domain filter is used.</p>
<b>User name</b>	<p>User name for connection to the JMX application (if required by your JMX application).</p>
<b>Password</b>	<p>Password for connection to the JMX application (if required by your JMX application).</p>
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, to wait for a response from the server before timing-out. After this time period passes, the monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 60 seconds (using a value other than the default timeout value may adversely affect performance)</p>
<b>Patterns &amp; Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Click the <b>Add New Counter</b>  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the <b>Delete Counter</b>  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the <b>View Matches for Selected Pattern Counter</b>  button to display counters that match the selected patterns.</p> <p><b>Note:</b> SiteScope uses Perl regular expressions for pattern matching. For example, if you enter <code>/cpu.*</code> or <code>cpu</code>, any counters with <code>cpu</code> in their name match this pattern and are added to the counters list.</p>



UI Element	Description
<b>Get Counters</b>	<p>Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated. For the list of counters that can be configured for this monitor, see "<a href="#">Monitor Counters</a>" below.</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>Counter Preview</b>	<p>Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.</p>
<b>Frequency of updating counters from server</b>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p><b>Default value:</b> 15 minutes</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The update frequency cannot be less than the monitor run frequency in Monitor Run Settings.</li> <li>• When configuring this setting in a template, the variable value can only be in time units of seconds.</li> <li>• Static counters are never deleted.</li> </ul>
<b>Continue displaying counters that no longer exist after update</b>	<p>When selected, counters that no longer exist after running the update mechanism to retrieve counters from the monitored server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful, for example, if a disk fails or for keeping track of counters that were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings on the next update.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> This option is relevant for dynamic counters only (those set using a regular expression). Static counters that are no longer available are still displayed even when this check box is cleared.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Hadoop cluster JMX exposes over 300 metrics.

Below are some of the most valuable metrics for monitoring the HDFS and MapReduce master nodes of the Hadoop cluster. For a more comprehensive list with descriptions, calculated counters, and default thresholds, see the Hadoop Solution Template Best Practices guide which can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope\_Hadoop\_Best\_Practices.pdf**.

**Note:** Each Hadoop cluster has a different size, workload, and job complexity. This means that you need to adjust the default threshold values according to your environment specifics, so as to maximize the benefits of the Hadoop monitor.

### HDFS Node Metrics

Hadoop/NameNode/FSNamesystemMetrics/CapacityRemainingGB  
Hadoop/NameNode/FSNamesystemMetrics/CapacityTotalGB  
Hadoop/NameNode/FSNamesystemMetrics/CapacityUsedGB  
Hadoop/NameNode/FSNamesystemMetrics/CorruptBlocks  
Hadoop/NameNode/FSNamesystemMetrics/ExcessBlocks  
Hadoop/NameNode/FSNamesystemMetrics/MissingBlocks  
Hadoop/NameNode/FSNamesystemMetrics/PendingDeletionBlocks  
Hadoop/NameNode/FSNamesystemMetrics/PendingReplicationBlocks  
Hadoop/NameNode/FSNamesystemMetrics/ScheduledReplicationBlocks  
Hadoop/NameNode/FSNamesystemMetrics/UnderReplicatedBlocks  
  
Hadoop/NameNode/FSNamesystemState/CapacityRemaining  
Hadoop/NameNode/FSNamesystemState/FSSState  
  
Hadoop/NameNode/jvm/gcCount Hadoop/NameNode/jvm/gcTimeMillis  
Hadoop/NameNode/jvm/memHeapCommittedM Hadoop/NameNode/jvm/memHeapUsedM  
Hadoop/NameNode/jvm/memNonHeapCommittedM Hadoop/NameNode/jvm/memNonHeapUsedM  
Hadoop/NameNode/jvm/threadsBlocked Hadoop/NameNode/jvm/threadsNew  
Hadoop/NameNode/jvm/threadsRunnable Hadoop/NameNode/jvm/threadsTerminated  
Hadoop/NameNode/jvm/threadsWaiting  
  
Hadoop/NameNode/NameNode/AddBlockOps Hadoop/NameNode/NameNode/blockReport\_avg\_time  
Hadoop/NameNode/NameNode/blockReport\_num\_ops Hadoop/NameNode/NameNode/fsImageLoadTime  
Hadoop/NameNode/NameNode/JournalTransactionsBatchedInSync  
  
Hadoop/NameNode/NameNodeInfo/NodesData/Dead nodes count  
Hadoop/NameNode/NameNodeInfo/NodesData/Decom nodes count  
Hadoop/NameNode/NameNodeInfo/NodesData/Live nodes count  
Hadoop/NameNode/NameNodeInfo/NodesData/NameDir statuses active count  
Hadoop/NameNode/NameNodeInfo/NodesData/NameDir statuses failed count  
Hadoop/NameNode/NameNodeInfo/PercentRemaining Hadoop/NameNode/NameNodeInfo/PercentUsed

### MapReduce Node Metrics

Hadoop/JobTracker/JobTrackerInfo/JobTrackerDetails/Alive nodes count  
Hadoop/JobTracker/JobTrackerInfo/JobTrackerDetails/Blacklisted nodes count  
Hadoop/JobTracker/JobTrackerInfo/JobTrackerDetails/Graylisted nodes count  
Hadoop/JobTracker/JobTrackerInfo/JobTrackerDetails/Total jobs count  
Hadoop/JobTracker/JobTrackerInfo/JobTrackerDetails/Total map slots  
Hadoop/JobTracker/JobTrackerInfo/JobTrackerDetails/Total nodes count  
Hadoop/JobTracker/JobTrackerInfo/JobTrackerDetails/Total reduce slots  
Hadoop/JobTracker/JobTrackerInfo/JobTrackerDetails/Used map slots  
Hadoop/JobTracker/JobTrackerInfo/JobTrackerDetails/Used reduce slots  
  
Hadoop/JobTracker/JobTrackerInfo/Queues Data/Queues in running state  
Hadoop/JobTracker/JobTrackerInfo/Queues Data/Queues in stopped state  
Hadoop/JobTracker/JobTrackerInfo/Queues Data/Queues in undefined state  
  
Hadoop/JobTracker/JobTrackerInfo/TaskTrackers/./Dir failures  
Hadoop/JobTracker/JobTrackerInfo/TaskTrackers/./Failures  
Hadoop/JobTracker/JobTrackerInfo/ThreadCount

Hadoop/JobTracker/JobTrackerMetrics/blacklisted\_maps  
Hadoop/JobTracker/JobTrackerMetrics/blacklisted\_reduces  
Hadoop/JobTracker/JobTrackerMetrics/heartbeats  
Hadoop/JobTracker/JobTrackerMetrics/jobs\_completed  
Hadoop/JobTracker/JobTrackerMetrics/jobs\_failed  
Hadoop/JobTracker/JobTrackerMetrics/jobs\_killed  
Hadoop/JobTracker/JobTrackerMetrics/jobs\_preparing  
Hadoop/JobTracker/JobTrackerMetrics/jobs\_running  
Hadoop/JobTracker/JobTrackerMetrics/jobs\_submitted  
Hadoop/JobTracker/JobTrackerMetrics/map\_slots  
Hadoop/JobTracker/JobTrackerMetrics/maps\_completed  
Hadoop/JobTracker/JobTrackerMetrics/maps\_failed  
Hadoop/JobTracker/JobTrackerMetrics/maps\_killed  
Hadoop/JobTracker/JobTrackerMetrics/maps\_launched  
Hadoop/JobTracker/JobTrackerMetrics/occupied\_map\_slots  
Hadoop/JobTracker/JobTrackerMetrics/occupied\_reduce\_slots  
Hadoop/JobTracker/JobTrackerMetrics/reduce\_slots  
Hadoop/JobTracker/JobTrackerMetrics/reduces\_completed  
Hadoop/JobTracker/JobTrackerMetrics/reduces\_failed  
Hadoop/JobTracker/JobTrackerMetrics/reduces\_killed  
Hadoop/JobTracker/JobTrackerMetrics/reduces\_launched  
Hadoop/JobTracker/JobTrackerMetrics/reserved\_map\_slots  
Hadoop/JobTracker/JobTrackerMetrics/reserved\_reduce\_slots  
Hadoop/JobTracker/JobTrackerMetrics/running\_maps  
Hadoop/JobTracker/JobTrackerMetrics/running\_reduces  
Hadoop/JobTracker/JobTrackerMetrics/trackers  
Hadoop/JobTracker/JobTrackerMetrics/trackers\_blacklisted  
Hadoop/JobTracker/JobTrackerMetrics/trackers\_decommissioned  
Hadoop/JobTracker/JobTrackerMetrics/trackers\_graylisted  
Hadoop/JobTracker/JobTrackerMetrics/waiting\_maps  
Hadoop/JobTracker/JobTrackerMetrics/waiting\_reduces

Hadoop/JobTracker/jvm/gcCount  
Hadoop/JobTracker/jvm/gcTimeMillis  
Hadoop/JobTracker/jvm/memHeapCommittedM  
Hadoop/JobTracker/jvm/memHeapUsedM  
Hadoop/JobTracker/jvm/memNonHeapCommittedM  
Hadoop/JobTracker/jvm/memNonHeapUsedM  
Hadoop/JobTracker/jvm/threadsBlocked  
Hadoop/JobTracker/jvm/threadsNew  
Hadoop/JobTracker/jvm/threadsRunnable  
Hadoop/JobTracker/jvm/threadsTerminated  
Hadoop/JobTracker/jvm/threadsTimedWaiting  
Hadoop/JobTracker/jvm/threadsWaiting

Hadoop/JobTracker/QueueMetrics.\*/jobs\_completed  
Hadoop/JobTracker/QueueMetrics.\*/jobs\_failed  
Hadoop/JobTracker/QueueMetrics.\*/jobs\_killed  
Hadoop/JobTracker/QueueMetrics.\*/jobs\_running  
Hadoop/JobTracker/QueueMetrics.\*/jobs\_submitted  
Hadoop/JobTracker/QueueMetrics.\*/maps\_completed  
Hadoop/JobTracker/QueueMetrics.\*/maps\_failed  
Hadoop/JobTracker/QueueMetrics.\*/maps\_killed  
Hadoop/JobTracker/QueueMetrics.\*/maps\_launched  
Hadoop/JobTracker/QueueMetrics.\*/reduces\_completed  
Hadoop/JobTracker/QueueMetrics.\*/reduces\_failed

```
Hadoop/JobTracker/QueueMetrics.*/reduces_killed  
Hadoop/JobTracker/QueueMetrics.*/reduces_launched  
Hadoop/JobTracker/QueueMetrics.*/reserved_map_slots  
Hadoop/JobTracker/QueueMetrics.*/reserved_reduce_slots  
Hadoop/JobTracker/QueueMetrics.*/waiting_maps  
Hadoop/JobTracker/QueueMetrics.*/waiting_reduces
```

## Tips/Troubleshooting

### General Notes

- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).
- The Hadoop monitor does not report the Hadoop Cluster CI type in the topology results. As a result, the default Hadoop cluster view does not show results reported by SiteScope.

### Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the **\_browsableContentMaxCounters** parameter in the **master.config** file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the **\_maxCountersForRegexMatch** parameter in the **master.config** file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The **\_maxCountersForRegexMatch** parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both **\_browsableContentMaxCounters** and **\_maxCountersForRegexMatch** parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

### Troubleshooting Logs

1. Check for dynamic framework errors in:
  - **<SiteScope root directory>\logs\dynamic\_monitoring\_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.

- **<SiteScope root directory>\logs\dynamic\_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).

To check for dynamic monitoring errors, copy the following section from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####
# Dynamic Monitoring
#####
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=false
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFileAppender
log4j.appender.dynamic.monitoring.appender.File=../${log.file.path}/dynamic_monitoring.log
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
```

2. Check for Hadoop monitor errors in:

- **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.
- **<SiteScope root directory>\logs\hadoop\_monitor.log**. This log provides information about Hadoop monitor errors.

To view Hadoop monitor errors, copy the following sections from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####
# Hadoop monitor
#####
log4j.category.com.mercury.sitescope.monitors.facades.HadoopMonitor=DEBUG, hadoop.appender
log4j.additivity.com.mercury.sitescope.monitors.facades.HadoopMonitor=false
log4j.category.com.mercury.sitescope.monitors.bigdata.hadoop.utils.HadoopMonitorUtils=DEBUG,
hadoop.appender
log4j.additivity.com.mercury.sitescope.monitors.bigdata.hadoop.utils.HadoopMonitorUtils=false

log4j.category.com.mercury.sitescope.monitors.bigdata.hadoop.tasks.HadoopMonitorCounterLoadingTask=
DEBUG, hadoop.appender

log4j.additivity.com.mercury.sitescope.monitors.bigdata.hadoop.tasks.HadoopMonitorCounterLoadingTask=
false

log4j.appender.hadoop.appender=org.apache.log4j.RollingFileAppender
log4j.appender.hadoop.appender.File=../${log.file.path}/hadoop_monitor.log
log4j.appender.hadoop.appender.MaxFileSize=${def.file.max.size}
log4j.appender.hadoop.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.hadoop.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.hadoop.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
log4j.appender.hadoop.appender.encoding=${general.encoding}
```

# Chapter 37: HAProxy Monitor

Use the HAProxy monitor to provide front- and back-end statistics to check that your HAProxy server is working properly. HAProxy is a solution that is used to provide high availability, load balancing, and proxying for TCP and HTTP-based applications. Using the HAProxy monitor provides a solution for monitoring infrastructures in the cloud.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HAProxy monitor.

## Learn About

### Supported Platforms/Versions

This monitor supports monitoring HAProxy 1.3, 1.4, and 1.5.10 on remote servers running on:

- Linux 2.4 on x86, x86\_64, Alpha, SPARC, MIPS, PARISC
- Linux 2.6 on x86, x86\_64, ARM (ixp425), PPC64
- Solaris 8/9 on UltraSPARC 2 and 3
- Solaris 10 on Opteron and UltraSPARC
- FreeBSD 4.10 - 8 on x86
- OpenBSD 3.1 to -current on i386, amd64, macppc, alpha, sparc64 and VAX (check the ports)

### Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

`http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080`

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

# Tasks

## How to Configure the HAProxy Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### HAProxy Monitor Settings

User interface elements are described below:

UI Element	Description
<b>URL</b>	URL of the stats-CSV report. <b>Example:</b> <code>http://server:port/haproxy?stats;csv</code>
<b>Credentials</b>	Option to use for authorizing credentials if the URL specified requires a name and password for access: <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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>Authorization user name</b>	User name to access the Web server stats page.
<b>Authorization password</b>	Password for accessing the Web server stats page.
<b>HTTP proxy</b>	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URL. Remember to include the port. <b>Example:</b> <code>proxy.thiscompany.com:8080</code>
<b>Proxy server user name</b>	Proxy user name if the proxy server requires a name and password to access the URL. <b>Note:</b> The proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	Proxy password if the proxy server requires a name and password to access the URL. <b>Note:</b> The proxy server must support Proxy-Authenticate for these options to function.



UI Element	Description
<b>Timeout (seconds)</b>	Number of seconds (between 1 and 120) that the monitor should wait for a response from the server before timing-out. After this time period passes, the monitor logs an error and reports an error status.  <b>Default value:</b> 60 seconds
<b>Counters</b>	Displays 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>	Opens the Select Counters Form, enabling you to select the counters you want to monitor.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Chapter 38: HP iLO (Integrated Lights-Out) Monitor

Use the HP iLO (Integrated Lights-Out) monitor that enables monitoring of hardware health on supported HP ProLiant servers. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch server health status and hardware configuration for stability monitoring and fast response for critical hardware issues. You can create a separate HP iLO Monitor instance for each supported server in your environment.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP iLO monitor.

## Learn About

This section includes:

- ["HP iLO Background" below](#)
- ["Supported Platforms/Versions" below](#)
- ["What to Monitor" on the next page](#)
- ["IPv6 Addressing" on the next page](#)
- ["License Consumption" on the next page](#)

## HP iLO Background

HP Integrated Lights-Out, or iLO, is an embedded server management technology exclusive to Hewlett-Packard but similar in functionality to the Lights out management (LOM) technology of other vendors.

iLO makes it possible to perform activities on an HP server from a remote location. iLO is currently available on all new ProLiant 300/500/blade server models and has a separate network connection (and its own IP address).

iLO actively participates in monitoring and maintaining server health, referred to as embedded health. iLO monitors temperatures in the server and sends corrective signals to the fans to maintain proper server cooling. In addition to temperature monitoring, iLO provides fan status monitoring and monitoring of the status of the power supplies, voltage regulators, and the internal hard drives.

System Information displays the health of the monitored system. These features are available without installing and loading the health driver for the installed operating system. The iLO microprocessor monitors these devices when the server is powered on during server boot, operating system initialization, and operation.

## Supported Platforms/Versions

The HP iLO monitor supports monitoring HP iLO 2, 3, and 4.

## What to Monitor

The HP iLO monitor makes use of performance counters to measure application server performance, and can be used to provide the following information:

- **Processors.** Displays the available processor slots and a brief status summary of the processor subsystem. If available, installed processor speed in MHz and cache capabilities are displayed.
- **Memory.** Displays the available memory slots and the type of memory, if any, installed in the slot.
- **Drives.** Displays the presence and condition of installed drive bays.
- **Power Supplies.** Displays the presence and condition of installed power supplies.
- **Voltage Regulator Modules (VRMs).** Displays VRM status. A VRM is required for each processor in the system. The VRM adjusts the power to meet the power requirements of the processor supported. A failed VRM prevents the processor from being supported and should be replaced.
- **Fans.** Displays the state of the replaceable fans in the server chassis. This data includes the area that is cooled by each fan and current fan speeds.
- **Temperatures.** Displays the temperature conditions monitored at sensors in various locations in the server chassis, and the processor temperature. The temperature is monitored to maintain the location temperature below the caution threshold. If the temperature exceeds the caution threshold, the fan speed is increased to maximum.
- **Other.** Other information about the server, such as firmware version and available slots.

## IPv6 Addressing

The HP iLO monitor supports IP version 6 addresses if the network and remote server support this protocol. For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

# Tasks

## How to Configure the HP iLO Monitor

### 1. Prerequisites

The following are important requirements for using the HP iLO monitor:

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- The HP iLO system administrator must configure the service on the ProLiant server so that it can access a command line interface over SSH.
- The configuration should be tested by connecting the server to the SSH client using the configured credentials, and running the following command:

```
show system1 -l 1
```

The result should contain targets and their properties available on the server.

2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### HP iLO Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	HP iLO server you want to monitor. Select a server from the server list (only those HP iLO remote servers that have been configured in SiteScope are displayed), or click <b>Add Remote Server</b> to add an HP iLO server.  <b>Note:</b> When working in template mode, 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.
<b>Add Remote Server</b>	Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.
<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>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see " <a href="#">Monitor Counters</a> " on the next page.  <b>Note:</b> 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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

The list of counters depends on the monitored system, and can differ significantly from system to system.

Below is a sample set of counters that are available:

<ul style="list-style-type: none"><li>• system1/firmware1/date</li><li>• system1/firmware1/version</li><li>• system1/cpu1/cachememory1</li><li>• system1/cpu1/cachememory2</li><li>• system1/cpu1/cachememory3</li><li>• system1/cpu1/speed</li><li>• system1/memory1/location</li><li>• system1/memory1/size</li><li>• system1/memory1/speed</li><li>• system1/slot1/type</li><li>• system1/slot1/width</li><li>• system1/fan1/DesiredSpeed</li><li>• system1/fan1/DeviceID</li><li>• system1/fan1/ElementName</li><li>• system1/fan1/HealthState</li><li>• system1/fan1/OperationalStatus</li><li>• system1/fan1/VariableSpeed</li><li>• system1/sensor1 : temp1/CurrentReading</li><li>• system1/sensor1 : temp1/DeviceID</li></ul>	<ul style="list-style-type: none"><li>• system1/sensor1 : temp1/ElementName</li><li>• system1/sensor1 : temp1/HealthState</li><li>• system1/sensor1 : temp1/OperationalStatus</li><li>• system1/sensor1 : temp1/RateUnits</li><li>• system1/sensor1 : temp1/SensorType</li><li>• system1/sensor1 : temp1/oemhp_CautionValue</li><li>• system1/sensor1 : temp1/oemhp_CriticalValue</li><li>• system1/powersupply1/ElementName</li><li>• system1/powersupply1/HealthState</li><li>• system1/powersupply1/OperationalStatus</li><li>• system1/properties/enabledstate</li><li>• system1/properties/name</li><li>• system1/properties/number</li><li>• system1/properties/oemhp_powerreg</li><li>• system1/properties/oemhp_pwracap</li><li>• system1/properties/oemhp_pwrmode</li><li>• system1/properties/oemhp_server_name</li><li>• system1/properties/processor_number</li><li>• system1/properties/pstate_number</li></ul>
--	--

## Tips/Troubleshooting

### General Tips/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- **Problem:** Intermittent issue with connection to HP-ILO remote server; periodically the Test Connection for this remote fails with a timeout error.

#### Solution:

1. Open the **master.config** file in **<SiteScope root directory>\groups**, and add the property `_hpILOConnectionDelay=200` (the value is measured in milliseconds).
2. Save the **master.config** file and restart SiteScope.

# Chapter 39: HP NonStop Event Log Monitor

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP NonStop Event Log monitor.

## Learn About

### Supported Platforms/Versions

- The minimum officially supported version of the HP NonStop Open System Management (OSM) Event Viewer is T0682 H02 ABU (released May 2009).
- All G-Series, H-Series, and J-Series NonStop RVUs are supported.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

## Tasks

### How to Configure the HP NonStop Event Log Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### HP NonStop Event Log Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>URL</b>	URL of the OSM Event Viewer. <b>Example:</b> https://<nonstopserver>:9991
<b>Match content</b>	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 Regular Expressions Overview in the Using SiteScope Guide. You can also use the Regular Expression Test tool to check your regular expressions. For details, see Regular Expression Tool in the Using SiteScope Guide.
<b>Timeout (seconds)</b>	Amount of time, in 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>	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>	Appropriate time zone, according to the location of the HP NonStop server.
<b>Filter Settings</b>	
<b>Event sources</b>	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. <b>Default value:</b> \$ZLOG
<b>Options</b>	Filter options. You can enter more than one option, using commas as separators. <b>Example:</b> CPU 0, PIN 253
<b>Owner</b>	Enter an owner in this field (up to 8 characters).
<b>Subsystem names</b>	Subsystem name. You can enter more than one subsystem, using commas as separators. <b>Example:</b> PATHWAY,TMF  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).

UI Element	Description
<b>Event IDs</b>	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.
<b>Filter files</b>	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.
<b>Authentication Settings</b>	
<b>Credentials</b>	<p>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 How to Configure Credential Preferences in the Using SiteScope Guide.</li> </ul>
<b>Pre-emptive authorization</b>	<p>Authorization user name and password option if SiteScope requests the target UR:</p> <ul style="list-style-type: none"> <li>• <b>Use global preference.</b> SiteScope uses 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> The user name and password are sent 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> The user name and password are sent 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 <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>Client side certificate</b>	<p>The certificate file, if using a client side certificate to access the target URL. 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>



UI Element	Description
<b>Client side certificate password</b>	Password if you are using a client side certificate and a password is required.
<b>Accept untrusted certificates for HTTPS</b>	Select 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 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>	Domain name and port of an HTTP Proxy Server if a proxy server can be used to access the URL.
<b>Proxy server user name</b>	Proxy server user name if the proxy server requires a name and password to access the URL. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	Proxy server password if the proxy server requires a name and password to access the URL. <b>Note:</b> Your proxy server must support Proxy-Authentication for these options to function.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Tips/Limitations

When configuring this monitor in template mode, you can use regular expressions to define counters.

# Chapter 40: HP NonStop Resources Monitor

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP NonStop Resources monitor.

## Learn About

This section includes:

- ["HP NonStop Resources Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["License Consumption" below](#)

## 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 *How to Configure SiteScope to Monitor a Remote UNIX Server* in the *Using SiteScope Guide*.

You can also use the Directory, Disk Space, Dynamic 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.

## Supported Platforms/Versions

All G-Series, H-Series, and J-Series NonStop RVUs are supported.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per object instance Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

# Tasks

## How to Configure the HP NonStop Resources Monitor

### 1. Prerequisites

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, Dynamic Disk Space, File, Log File, or Script monitor), you must perform the following on the HP NonStop Operating System server:

- a. Create a user for SiteScope monitoring.
- b. In the **/etc/profile** and **.profile** files, perform the following:
  - Comment out the string: `set -o vi.`
  - Set the following parameter: `export PS1='$PWD:`

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.



**Note:** 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 **tac1**.
- 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>`.

# UI Descriptions

## HP NonStop Resources Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>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>Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details (in the <b>Operating System</b> list, you must select <b>NonStopOS</b>). For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Available Counters</b>	<p>Displays the available measurements for this monitor.</p> <p>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> <p><b>Note:</b></p> <ul style="list-style-type: none"><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>• When configuring this monitor in template mode, you can use regular expressions to define counters.</li></ul> <p>For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<b>CPU</b> <ul style="list-style-type: none"><li>• PROCESSBUSYTIME</li><li>• INTERRUPT TIME</li><li>• IDLE TIME</li></ul> <b>Memory</b> <ul style="list-style-type: none"><li>• ALLOCS (per sec)</li><li>• DISKREADS (per sec)</li><li>• DISKWRITES (per sec)</li><li>• FAULTS (per sec)</li><li>• FREE (16KB pages)</li><li>• FREEMIN (16KB pages)</li></ul>	<ul style="list-style-type: none"><li>• FREEQUOTA (16KB pages)</li><li>• FREERED (16KB pages)</li><li>• LOCKED (16KB pages)</li><li>• LOCKED (KSEG0) (16KB pages)</li><li>• MUTEXCRAX (per sec)</li><li>• NONMUTEXCRAX (per sec)</li><li>• PHYSCL (16KB pages)</li><li>• REDBUSY (per sec)</li><li>• REDHIT (per sec)</li><li>• REDTASK (per sec)</li><li>• SWAPBL (16KB pages)</li><li>• UNDUMPED (16KB pages)</li></ul>
---	---

# Chapter 41: HP Vertica JDBC Monitor

The HP Vertica JDBC monitor enables you to dynamically monitor the health and performance statistics of key items of the Vertica cluster infrastructure. The monitor gets counters from a Vertica cluster that provides access to its statistics by using a JDBC driver. Vertica can be monitored by SNMP trap and System tables.

This monitor is designed to manage large, fast-growing volumes of data and provide fast query performance when used for data warehouses and other query-intensive applications. Using this monitor, you can select specific measurements or use the dynamic monitoring mechanism to automatically update counters and thresholds that changed in Vertica system tables during run-time.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of the Vertica cluster infrastructure. For details, see HP Vertica Solution Template in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP Vertica JDBC monitor.

## Learn About

This section includes:

- ["Vertica JDBC Monitor Overview" below](#)
- ["Supported Platforms/Versions" on the next page](#)
- ["Setup Requirements and User Permissions" on the next page](#)
- ["HP Vertica JDBC Topology" on the next page](#)
- ["License Consumption" on page 312](#)

## Vertica JDBC Monitor Overview

This monitor enables you to:

- Monitor specific counters on a Vertica cluster using static counters. You can monitor multiple parameters or counters with a single monitor instance.
- Select the counter patterns you want to monitor using a regular expression or a static string, and let the monitor dynamically update Vertica counters that match the pattern defined by the regular expression. Dynamic monitoring enables you to configure the monitor on a one time basis, and leave it to update itself.

When configuring a dynamic monitor, you can define a counter pattern that specifies the counters you want to monitor. The monitor scans the target host periodically, and creates the counters that are aligned with the given counter pattern.

If a new Vertica counter is added to the machine and part or all of its counters correspond to the counter pattern, the counters that match the counter pattern are automatically added to the monitor when the counters are next updated from the server. Similarly, if a Vertica counter that corresponds to the counter pattern is no longer available, counters for that metric are removed from the monitor (unless you choose not to delete them, in which case they are still displayed in the monitor's counter list).

You can also define the required thresholds for the counter's pattern. In this way, thresholds are also updated automatically when the counters are updated.

For more details on the dynamic monitoring mechanism, see *Dynamic Monitoring Mechanism* in the *Using SiteScope Guide*.

## Supported Platforms/Versions

The HP Vertica monitor supports monitoring on Vertica 6.0.1, 6.1, 7.0, 7.1.1.

## Setup Requirements and User Permissions

The following are several key requirements for using the HP Vertica JDBC monitor:

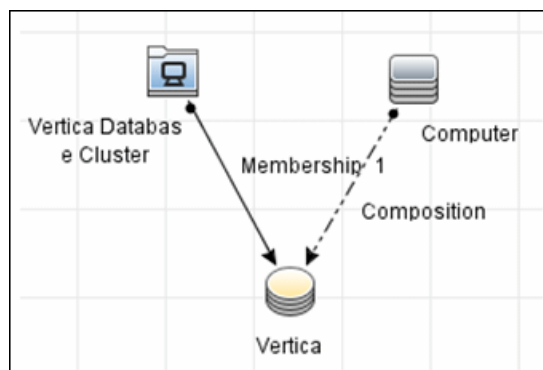
- You should download the Vertica JDBC driver from the official HP Vertica site and copy it to the **<SiteScope root directory>\WEB-INF\lib** subdirectory.

**Tip:** Many database driver packages are available as compressed (zipped) archive files or .jar files. If the file is in zip format, unzip the contents to a temporary directory. Stop and restart the SiteScope service after copying the driver file to the SiteScope machine.

- The syntax for accessing the database driver is:  
`jdbc:vertica://<Vertica_host>:<port_number>/<database_name>`  
For details, see the [HP Vertica Analytics Platform Version 6.1.x Documentation](https://my.vertica.com/docs/6.1.x/HTML/index.htm) (<https://my.vertica.com/docs/6.1.x/HTML/index.htm>).
- Generally, only one instance of each type of JDBC driver client should be 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 Vertica JDBC drivers from two different versions of Vertica is unlikely to work.
- You must have a database user login that SiteScope can use to access the database. SiteScope is only able to run the SQL queries that this user has permission to run on the database.

## HP Vertica JDBC Topology

The HP Vertica JDBC monitor can identify the topology of the database system being monitored. If **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting), the monitor creates the following topology in BSM's RTSM.



For information about retrieving topologies and reporting them to BSM, see *Reporting Discovered Topologies to BSM* in the *Using SiteScope Guide*.

**Note:** Topology reporting for this monitor is only supported in BSM 9.23 and later.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitored group.  A group is a path in the tree (not containing the counter name itself) for which at least one direct counter is selected).	HP Vertica JDBC monitor consumes one OS instance per monitored server and one OS instance per monitored node.  Note: This monitor is not available with Community Edition.


## Tasks

### How to Configure the HP Vertica JDBC Monitor

#### 1. Prerequisites

Before configuring the monitor, make sure you have the necessary requirements and permissions. For details, see ["Setup Requirements and User Permissions" on the previous page](#).

#### 2. Configure the monitor properties

- Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **HP Vertica JDBC**. The New HP Vertica JDBC Monitor dialog box opens.
- In the General Settings panel, enter a name and description for the monitor.
- In the HP Vertica JDBC Monitor Settings panel, enter the URL of the Vertica cluster you want to monitor, the driver to which you want to connect, and use credentials. For user interface details, see the UI Descriptions section below.
- In the **Patterns & Counter** section, click the **Get Counter** button, and select the counters you want to monitor from the Select Counters Form (the form displays static counters only). The counters are added to the Counter Preview tree.
- For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
  - Clicking the **Add New Counter**  button to add an empty line to the table, and then by creating a pattern format using a regular expression.

#### Tip:

- The pattern should always start and end with the forward slash ("/") character.
- Special characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character).
- Use ".\*" to describe any character any number of times.


For example, `/Query Metrics/.*/`, shows all query metrics.

- Selecting a static counter, and editing the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions Overview in the



Using SiteScope Guide.

**Note:** For details on the maximum number of counters that can be selected from the browsable tree and the maximum number of counters that can match the selected counter patterns when creating and updating dynamic monitors, see ["Tips/Troubleshooting" on page 318](#). If the maximum number of counters that can be deployed is exceeded, an error is written to the **RunMonitor.log**.

- f. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counter Preview tree.
- g. Set the frequency for updating counters from the server in the **Frequency of updating counters from server** box. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- h. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful for keeping track of the counters that were previously being monitored.
- i. Click **Verify & Save** or **Save** to save your settings.
- j. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

**Note:** When configuring threshold settings for the HP Vertica JDBC monitor:

- The monitor **always(default)** counter configured in the **Good if** section of the monitor's properties means that the state of the monitor is good, unless one of the thresholds of any of the other counters is breached.
- The **countersinError** counter configured in the **Error if** section of the monitor's properties means that the state of the monitor is error if one of the other counters is unavailable.

**Tip:** The **Database Connection Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Database Connection Tool\ in the Using SiteScope Guide.

### 3. Enable topology reporting - optional

- To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide. For details on the HP Vertica JDBC monitor topology, see ["HP Vertica JDBC Topology" on page 311](#).
- To see topology reported by the monitor and Health Indicators assigned to monitor metrics, you should download and install the following resources from the HPE Live Network:

#### Content Pack for DDM:

- i. Navigate to **HPE Live Network Home > Discovery and Dependency Mapping > Content Packs for DDM > Content Files** (<https://hpln.hp.com/node/31/contentfiles>).

- ii. In the resources tree, select: **Downloads > Content Packs for UCMDB 9.03 – 9.05 > DDM Content Pack 11 > Technology Specific Content**.
- iii. Download the **Vertica** zip file and the installation instructions PDF.
- iv. Follow the instructions in the PDF for importing the content package into RTSM.

**Content Pack for BSM:**

- i. Navigate to **HPE Live Network Home > Business Service Management > Content Packs for BSM > Content Files** (<https://hpln.hp.com/node/12361/contentfiles>).
- ii. In the resources tree, select: **Downloads > Content > Vertica > 9.22**.
- iii. Download the zip file corresponding your BSM platform and the installation instructions PDF
- iv. Follow the instructions in the PDF for installing the content pack.

#### 4. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the Vertica database where the performance counters you want to monitor are running and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:




- The SiteScope **Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

## UI Descriptions

### HP Vertica JDBC Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Database connection URL</b>	Connection URL to the Vertica cluster you want to monitor. The syntax is <code>jdbc:vertica://&lt;host&gt;:&lt;port&gt;/&lt;database&gt;</code> .
<b>Database driver</b>	Driver used to connect to the Vertica database. <b>Example:</b> <code>com.vertica.jdbc.Driver</code>

UI Element	Description
<b>Credentials</b>	<p>Option for providing the user name and password to be used to access the Vertica 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 How to Configure Credential Preferences in the Using SiteScope Guide.</li> </ul>
<b>Patterns &amp; Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Click the <b>Add New Counter</b>  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the <b>Delete Counter</b>  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the <b>View Matches for Selected Pattern Counter</b>  button to display counters that match the selected patterns.</p> <p><b>Note:</b> SiteScope uses Perl regular expressions for pattern matching. For example, if you enter <code>/query.* /</code> or <code>query</code>, any counters with <code>query</code> in their name match this pattern and are added to the counters list.</p>
<b>Get Counters</b>	<p>Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</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>Counter Preview</b>	<p>Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.</p>

UI Element	Description
<b>Frequency of updating counters from server</b>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p><b>Default value:</b> 15 minutes</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>The update frequency cannot be less than the monitor run frequency in Monitor Run Settings.</li> <li>When configuring this setting in a template, the variable value can only be in time units of seconds.</li> <li>Static counters are never deleted.</li> </ul>
<b>Continue displaying counters that no longer exist after update</b>	<p>When selected, counters that no longer exist after running the update mechanism to retrieve counters from the monitored server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful, for example, if a disk fails or for keeping track of counters that were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings on the next update.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> This option is relevant for dynamic counters only (those set using a regular expression). Static counters that are no longer available are still displayed even when this check box is cleared.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of default counters for this monitor grouped by specified table columns:

Tree Branch	Counters
Active Events	Event Code, Event Description for each node
Backups	Snapshot Name, Backup Timestamp, Epoch, Node Count, Objects for each node
Configuration Parameters	Value and Default Value for each configuration parameter
Critical Hosts	List of critical hosts
Critical Nodes	List of critical nodes

Tree Branch	Counters
Disk Resource Rejections	Rejected Reason, Rejected Count for each resource type on each node if specified rejection was occurred
Disk Storage	Storage Usage, Rank, Throughput, Latency, Storage Status, Disk Block Size (bytes), Disk Space Used (Blocks), Disk Space Used (MB), Disk Space Free (Blocks), Disk Space Free (MB), Disk Space Free % for each storage path on each node
Host Resources	Open Files Limit, Threads Limit, Core File Limit Max Size (bytes), Processor Count, Processor Core Count, Processor Description, Opened File Count, Opened Socket Count, Opened Nonfile Nonsocket Count, Total Memory (bytes), Total Memory Free(bytes), Total Buffer Memory (bytes), Total Memory Cache (bytes), Total Swap Memory (bytes), Total Swap Memory Free (bytes), Disk Space Free (MB), Disk Space Used (MB), Disk Space Total (MB) on each host
Locks	Lock Duration (sec) for each locked object on each node if lock is longer than 60 sec
Nodes	Node State, Node Address, Export Address, Is Ephemeral for each node
Node Resources	Host Name, Process Size (bytes), Process Resident Set Size (bytes), Process Shared Memory Size (bytes), Process Text Memory Size (bytes), Process Data Memory Size (bytes), Process Library Memory Size (bytes), Process Dirty Memory Size (bytes), Spread Host, Node Port, Data Port on each node
Projections	Verified Fault Tolerance, Is Up To Date, Has Statistics for each projection
Query Metrics	Active User Session Count, Active System Session Count, Total User Session Count, Total System Session Count, Total Active Session Count, Total Session Count, Running Query Count, Executed Query Count on each node
Query Performance	Number of Running Queries, Longest Query, Longest Query Duration (sec) on each node
Recovery Status	Recover Epoch, Recovery Phase, Splits Completed, Splits Total, Historical Completed, Historical Total, Current Completed, Current Total, Is Running on each node
Resource Pools	Is Internal, Memory Size, Max Memory Size, Execution Parallelism, Priority, Runtime Priority, Runtime Priority Threshold, Queue Timeout, Planned Concurrency, Max Concurrency, Runtime Cap, Single Initiator for each exists resource pool
Resource Pool Status	Is Internal, Memory Size (KB), Memory Size Actual (KB), Memory In Use (KB), General Memory Borrowed (KB), Queueing Threshold (KB), Max Memory Size (KB), Running Query Count, Planned Concurrency, Max Concurrency, Is Standalone, Queue Timeout (sec), Execution Parallelism, Priority, Runtime Priority, Runtime Priority Threshold, Single Initiator, Query Budget (Kb) for each exists resource pool on each node
Resource Queue	Queue Length, Memory Requested (KB) for each pool on each node if queue exists
Resource Rejections	Rejection Count for each reason for each resource type on each node if rejection was occurred

Tree Branch	Counters
Resource Usage	Request Count, Local Request Count, Request Queue Depth, Active Thread Count, Open File Handle Count, Memory Requested (KB), Address Space Requested (KB), WOS Used Bytes, WOS Row Count, ROS Used (bytes), ROS Row Count, Total Row Count, Total Used (bytes), Resource Request Reject Count, Resource Request Timeout Count, Resource Request Cancel Count, Disk Space Request Reject Count, Failed Volume Reject Count, Tokens Used, Tokens Available on each node
Storage Tiers	Node Count, Location Count, ROS Container Count, Total Occupied Size for each storage location
System	Current Epoch, AHM Epoch, Last Good Epoch, Refresh Epoch, Designed Fault Tolerance, Node Count, Node Down Count, Current Fault Tolerance, Catalog Revision Number, WOS Used (bytes), WOS Row Count, ROS Used (bytes), ROS Row Count, Total Used (bytes), Total Row Count
System Resource Usage	Average Memory Usage %, Average CPU Usage %, Network RX (KBytes Per Second), Network TX (KBytes Per Second), IO Read (KBytes Per Second), IO Written (KBytes Per Second) on each node
System Services	Service Type, Service Group, Service Interval (sec), Is Enabled, Last Run Start, Last Run End for each service on each node
WOS Container Storage	Region Virtual Size (KB), Region Allocated Size (KB), Region In Use Size (KB), Region Small Release Count, Region Big Release Count, Extra Reserved (bytes), Extra Used (bytes) for each WOS Allocation Region for each WOS type on each node

## Tips/Troubleshooting

### General Tips/Limitations

- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).

### Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the `_browsableContentMaxCounters` parameter in the `master.config` file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the `_maxCountersForRegexMatch` parameter in the `master.config` file. If during deployment,

the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The **\_maxCountersForRegexMatch** parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both **\_browsableContentMaxCounters** and **\_maxCountersForRegexMatch** parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

## Troubleshooting Logs

1. Check for dynamic framework errors in:

- **<SiteScope root directory>\logs\dynamic\_monitoring\_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
- **<SiteScope root directory>\logs\dynamic\_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).

To check for dynamic monitoring errors, copy the following section from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####
# Dynamic Monitoring
#####
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=false
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFileAppender
log4j.appender.dynamic.monitoring.appender.File=./${log.file.path}/dynamic_monitoring.log
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
#####
```

2. Check for HP Vertica JDBC monitor errors in:

- **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.
- **<SiteScope root directory>\logs\vertica\_monitor.log**. This log provides information about HP Vertica JDBC monitor errors.

To view HP Vertica JDBC monitor errors, copy the following sections from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####
# HP Vertica Monitor
#####
log4j.category.com.mercury.sitescope.monitors.facades.VerticaJDBCMonitor=DEBUG, vertica.appender
log4j.additivity.com.mercury.sitescope.monitors.facades.VerticaJDBCMonitor=false
#####
```

```
log4j.category.com.mercury.sitescope.monitors.vertica=DEBUG, websphere.appender
log4j.additivity.com.mercury.sitescope.monitors.vertica=false
log4j.appender.vertica.appender=org.apache.log4j.RollingFileAppender
log4j.appender.vertica.appender.File=./${log.file.path}/vertica_monitor.log
log4j.appender.vertica.appender.MaxFileSize=${def.file.max.size}
log4j.appender.vertica.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.vertica.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.vertica.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
log4j.appender.vertica.appender.encoding=${general.encoding}
```



# Chapter 42: IPMI Monitor

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 affect availability and degrade performance. Create a separate monitor instance for each server you are running.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the IPMI monitor.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric (Maximum: 120)	One OSi license per monitored host.

# Tasks

## How to Configure the IPMI Monitor

### 1. Prerequisites

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.

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## IPMI Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server name</b>	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>	Port number of the IPMI device. <b>Default value:</b> 623
<b>Credentials</b>	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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>Counters</b>	Displays the server performance counters to check with this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to 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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Measures various hardware metrics even if the operating system is unresponsive. The list of available counters is vendor dependant and usually includes CPU and system temperature, system fans RPM, CPU and system voltage and more.

# Tips/Troubleshooting

## General Tips/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 43: JMX Monitor

This monitor enables you to monitor the performance statistics of those Java-based applications that provide access to their statistics by using the standard JMX remoting technology defined by JSR 160 (remote JMX).

## Note:

- There is also a ["Dynamic JMX Monitor" on page 236](#) which enables you to select the counter patterns you want to monitor using a regular expression, and the monitor dynamically updates MBean counters that match the pattern. Dynamic monitoring enables you to configure the monitor on a one time basis, and leave it to update itself.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the JMX monitor.

## Learn About

This section includes:

- ["JMX Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Applications Supporting JSR 160" on page 325](#)
- ["WebLogic Application Server Topology" on page 326](#)
- ["Thread Pool Settings" on page 326](#)
- ["License Consumption" on page 327](#)

## JMX Monitor Overview

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:

- When monitoring a WebLogic Application Server using a t3 or t3s protocol, you need to use WebLogic's own protocol provider package. For details on how to use the t3 or t3s protocol, see ["How to monitor a WebLogic 11g \(10.3.1-10.3.5\) or 12c server with an SSL connection using the t3, t3s, iiop or iiops protocol" on page 328](#).
- SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of a WebLogic Application server. For details, see WebLogic Solution Templates in the Using SiteScope Guide.

## Supported Platforms/Versions

This monitor supports monitoring on:

- WebLogic 11g (10.3.1-10.3.5), 12c

**Note:** Monitoring WebLogic 9.x and 10.x is no longer supported due to different Java versions run by SiteScope 11.2x or later, and WebLogic Application Server 9.x and 10.x.

- Apache Tomcat 5.0, 5.5, 6.0, 6.0.33, 7.0.25, 7.0.50, 7.0.61, 7.0.62, 8.0.23
- Oracle Application Server 10.1.3g
- JBoss servers 4.0.3, 4.2, 5.0, 5.1, 6.0, 6.1, 7.0, 7.1.x
- JBoss EAP 6.1.x - 6.2.x, 6.3.0
- Sun Glassfish Enterprise Server 2.1, 3.1
- WildFly 8.0.0, 8.1.0, 8.2.0

## Applications Supporting JSR 160

Here are some applications that currently support JSR 160 and information about how to monitor them:

- Oracle WebLogic 11g (10.3.1-10.3.5) and 12c support JSR 160, which can be enabled on the WebLogic application server by following instructions found on the [Oracle Web site](http://download.oracle.com/docs/cd/E14571_01/apirefs.1111/e13952/taskhelp/channels/EnableAndConfigureIIOP.html) ([http://download.oracle.com/docs/cd/E14571\\_01/apirefs.1111/e13952/taskhelp/channels/EnableAndConfigureIIOP.html](http://download.oracle.com/docs/cd/E14571_01/apirefs.1111/e13952/taskhelp/channels/EnableAndConfigureIIOP.html)).

Once enabled, the JMX URL for monitoring the server follows the following form:

```
service:jmx:iiop://<host>:<port>//jndi/weblogic.management.mbeanservers.  
runtime  
or
```

```
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 11g (10.3.1-10.3.5) and 12c servers, see ["How to create a JMX Monitor for a WebLogic Server" on page 327](#).

- Tomcat 5.x and 6.0 support 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 [Oracle Web site](http://download.oracle.com/javase/1.5.0/docs/guide/jmx/tutorial/security.html) for more details (<http://download.oracle.com/javase/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.

- JBoss 4.0.3 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  
-Djboss.platform.mbeanserver  
-Djavax.management.builder.initial=org.jboss.system.server.jmx.  
MBeanServerBuilderImpl
```

- JBoss 6.1 supports JSR 160, by defining the following properties to the JVM on startup:

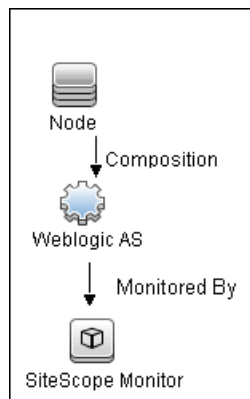
```
-Dcom.sun.management.jmxremote  
-Dcom.sun.management.jmxremote.port=9999  
-Dcom.sun.management.jmxremote.authenticate=false  
-Dcom.sun.management.jmxremote.ssl=false  
-Djboss.platform.mbeanserver  
-Djavax.management.builder.initial=org.jboss.system.server.jmx.  
MBeanServerBuilderImpl  
-Djava.endorsed.dirs="%JBASS_ENDORSED_DIRS%"  
-classpath "%JBASS_CLASSPATH%" org.jboss.Main %*
```

- 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) (<http://www.jcp.org/en/jsr/detail?id=160>).

## WebLogic Application Server Topology

The JMX monitor can identify the topology of WebLogic Application Servers. If **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting), the monitor creates the following topology in BSM's RTSM.



### Note:

- By default, the JMX monitor reports topology data to BSM when monitoring the WebLogic application server only. To report topology data when monitoring any other environment (such as JBoss or Oracle), you need to type the server name and hostname into the CI type key attributes fields in **HP Integration Settings > Topology Settings**.
- When the JMX monitor reports topology for a WebLogic cluster, if all counters in the monitor belong to one server, SiteScope reports the server name to BSM. Where all counters in the monitor are from different servers, SiteScope reports the server cluster name to BSM.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

## Thread Pool Settings

The JMX monitor has two modes for using thread pools: regular mode which uses the existing threads to bring information (counter names and values) from the JMX server, and sandbox mode which uses additional threads taken from thread pool. By default, the JMX monitor uses the regular mode. If you supply additional classpath, the default is sandbox mode. To enable the monitor to use a separate thread pool (sandbox mode) even when not using additional classpath, set the `_disableExtraClassPathExecutor` parameter to `=false` in the `<SiteScope root directory>\groups\master.config` file.

You can configure JMX thread pool settings in **Preferences > Infrastructure Preferences > Monitor Settings**. These settings are only relevant when using a separate thread pool (sandbox mode). These settings are for each thread pool. A new thread pool is created for each additional classpath used by the JMX monitor. The same thread pool is used for all JMX monitors that do not use additional classpath, and for all JMX monitors that use additional classpath if `_disableExtraClassPathExecutor` is set to `=false`.

- **JMX thread pool core size:** Number of threads to keep in the JMX pool that can be created for JMX tasks, even if they are idle. The default value is 10.
- **JMX thread pool idle time (seconds):** When the number of threads is greater than the core, this is the

maximum time that excess idle threads will wait for new JMX tasks before timing out. The default value is 30 seconds.

- **JMX thread pool maximum size:** Maximum number of threads allowed in the pool. If the number of threads in the pool is greater than the core but less than the maximum, and the queue is full, then new threads will be created for the JMX tasks until the maximum number of threads in pool is reached. The default value is 200.
- **JMX thread pool queue size:** Maximum number of JMX tasks that can be added to the queue. If all the core threads are busy now, the new tasks will be added to queue until the max queue size is reached. The default value is 400.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

## Tasks

This section includes the following tasks:

- ["How to create a JMX Monitor for an Apache Tomcat, JBoss, Sun Glassfish Enterprise, Oracle Application Server, or WildFly" below](#)
- ["How to create a JMX Monitor for a WebLogic Server" below](#)
- ["How to monitor a WebLogic 11g \(10.3.1-10.3.5\) or 12c server with an SSL connection using the t3, t3s, iiop or iiops protocol" on the next page](#)

### How to create a JMX Monitor for an Apache Tomcat, JBoss, Sun Glassfish Enterprise, Oracle Application Server, or WildFly

Configure the monitor properties as described in the UI Descriptions section below.

**Note:** To get counters from a JBoss 7.1.x, JBoss EAP 6.1.x - 6.2.x, or WildFly 8.0.0 server, you must:

1. Add the following jars to classpath:
  - **jboss-common-core.jar**
  - **jboss-client.jar**
2. Select the **Load additional classpath first** check box.

### How to create a JMX Monitor for a WebLogic Server

1. To monitor a WebLogic 11g (10.3.1-10.3.5) or 12c server, create a JMX monitor, and enter the following in the **JMX URL** box:

```
service:jmx:iiop://<host>:<port>//jndi/weblogic.management.mbeanservers.  
runtime  
or
```

```
service:jmx:iiop:///jndi/iiop://<host>:<port>/weblogic.management.  
mbeanservers.runtime
```

2. (For WebLogic 6.x, 7.x, and 8.x) To help you to select the counters that you require, you can open a WebLogic monitor for versions prior to WebLogic 9.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.
3. (For WebLogic 11g or 12c) Enter the **wfullclient.jar** in the **Additional Classpath** field in the JMX Monitor Settings. You can specify the timeout for JMX task execution (mbeans retrieval and conversion into xml) by modifying the **\_overallJMXCountersRetrievalTimeout** property in the **master.config** file. The default value is 15 minutes. This is not an ORB timeout.

**Note:** For details on creating the **wfullclient.jar**, refer to the Oracle documentation on Using the WebLogic JarBuilder Tool ([http://download.oracle.com/docs/cd/E12840\\_01/wls/docs103/client/jarbuilder.html](http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html)).

4. Configure user credentials as required  
You only need to specify a **User name** and **Password** if you do not want to use the default setup for iiop. If you leave these fields blank (recommended), WebLogic uses the default iiop user credentials that have already been configured in the WebLogic application.  
You must also configure the security realm of WebLogic to exactly match the configured user credentials (if specified), or the iiop user credentials (if the **User name** and **Password** fields are left blank).
5. Configure the other monitor properties as required  
Configure the other properties as described in the UI Description section below.
6. Enable topology reporting - optional  
To enable topology reporting for WebLogic Application Servers, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "[WebLogic Application Server Topology](#)" on page 326.  
For user interface details, see BSM Integration Data and Topology Settings in the Using SiteScope Guide.

## How to monitor a WebLogic 11g (10.3.1-10.3.5) or 12c server with an SSL connection using the t3, t3s, iiop or iiops protocol

When monitoring a WebLogic Application Server using a t3, t3s, iiop or iiops protocol, you need to use WebLogic's own protocol provider package.

**Note:** When monitoring a WebLogic server with the Administration port enabled, the t3s protocol must be used.

1. Enter the URL in the following format in the **JMX URL** box of JMX Monitor Settings:

- **For t3 protocol:**

```
service:jmx:t3://<host>:<port>/jndi/weblogic.management.  
mbeanservers.runtime  
where the default port for t3 protocol is 7001
```

- **For t3s protocol:**

```
service:jmx:t3s://<host>:<port>/jndi/weblogic.management.  
mbeanservers.runtime  
where the default port for t3s protocol is 7002
```



- **For iiop protocol:**

```
service:jmx:iiop://<host>:<port>//jndi/weblogic.management.mbeanservers.  
runtime  
or
```

```
service:jmx:iiop:///jndi/iiop://<host>:<port>/weblogic.management.  
mbeanservers.runtime
```

- **For iiops protocol:**

```
service:jmx:iiops://host:port/jndi/weblogic.management.  
mbeanservers.runtime
```

2. (For t3 or t3s protocols) Copy the following jars from the WebLogic library to any folder on the SiteScope server:

- %WEBLOGIC\_HOME%\server\lib\wlclient.jar
- %WEBLOGIC\_HOME%\server\lib\wljmxclient.jar
- %WEBLOGIC\_HOME%\server\lib\weblogic.jar
- %WEBLOGIC\_HOME%\server\lib\wlfullclient.jar
- %WEBLOGIC\_HOME%\server\lib\weblogicclient+ssl.jar (for t3s protocol only)
- %WEBLOGIC\_HOME%\server\lib\cryptoj.jar (for t3s protocol only, if this file is present in WebLogic library)

Specify the full path to the copied jars in the **Additional Classpath** field in the JMX Monitor Settings separated by “,”.

**Note:** For details on creating the **wlfullclient.jar**, refer to the Oracle documentation on Using the WebLogic JarBuilder Tool ([http://download.oracle.com/docs/cd/E12840\\_01/wls/docs103/client/jarbuilder.html](http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html)).

3. (For iiop or iiops protocols) Copy the following jars from the WebLogic library to any folder on the SiteScope server:

- %WEBLOGIC\_HOME%\server\lib\wlfullclient.jar
- %WEBLOGIC\_HOME%\server\lib\wlcipher.jar (for iiops protocol only)

Specify the full path to **wlfullclient.jar** in the **Additional Classpath** field in the JMX Monitor Settings.

For details on creating the **wlfullclient.jar**, refer to the Oracle documentation on Using the WebLogic JarBuilder Tool ([http://download.oracle.com/docs/cd/E12840\\_01/wls/docs103/client/jarbuilder.html](http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html)).

4. (For t3s and iiops protocols) Enable SSL on the WebLogic server and import the SSL certificate into the SiteScope keystore. For details, see Certificate Management Overview.
5. Configure the other monitor settings as required.  
For details, see Settings Common to All Monitors in the Using SiteScope Guide.



# UI Descriptions

## JMX Monitor Settings

User interface elements are described below:

UI Element	Description
JMX URL	<p>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></p> <ul style="list-style-type: none"><li>When creating a JMX monitor for a WebLogic 11g or 12c server, enter the following URL: <code>service:jmx:iiop://&lt;host&gt;:&lt;port&gt;//jndi/weblogic.management.mbeanservers.runtime</code> or <code>service:jmx:iiop:///jndi/iiop://&lt;host&gt;:&lt;port&gt;/weblogic.management.mbeanservers.runtime</code></li><li>When creating a JMX monitor for a JBoss server, your system administrator should configure the JBoss server, and then report which ports are enabled for JMX access.</li><li>When creating a JMX monitor for a JBoss 7.1.x or JBoss EAP 6.1.x - 6.2.x server, enter the following URL: <code>service:jmx:remoting-jmx://&lt;host&gt;:&lt;port&gt;</code></li><li>When creating a JMX monitor for a WildFly 8.0.0 server, enter the following URL: <code>service:jmx:http-remoting-jmx://&lt;host&gt;:&lt;port&gt;</code></li><li>If you are using a t3 or t3s protocol, you need to use WebLogic's own protocol provider package and the JMX URL is in a different format. For details, see <a href="#">"How to monitor a WebLogic 11g (10.3.1-10.3.5) or 12c server with an SSL connection using the t3, t3s, iiop or iiops protocol"</a> on page 328.</li><li>The JMX over RMI protocol is not firewall friendly.</li></ul>

UI Element	Description
<b>Domain filter</b>	<p>Domain filter to show only those counters existing within a specific domain (optional). This filter does not have full regular expression support.</p> <p>You can specify the domain name or full path to MBean. The full path can be taken from the MBean objectName property using JConsole.</p> <p><b>Example:</b> Note that these MBean examples have different node properties in the path: type-host-path in the first and type-resourcetype-name in the second.</p> <ul style="list-style-type: none"> <li>For MBean "Catalina/Cache/localhost/SiteScope" specify: "Catalina:type=Cache,host=localhost,path=/SiteScope"</li> <li>For MBean "Catalina/Environment/Global/simpleValue" specify: "Catalina:type=Environment,resourcetype=Global,name=simpleValue"</li> </ul>
<b>User name</b>	User name for connection to the JMX application (if required by your JMX application).
<b>Password</b>	Password for connection to the JMX application (if required by your JMX application).
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, to wait for a response from the server before timing-out. After this time period passes, the monitor logs an error and reports an error status.</p> <p><b>Default value:</b> 60 seconds (using a value other than the default timeout value may adversely affect performance)</p>
<b>Additional Classpath</b>	<p>Specify the classpath library that is used to resolve unknown classes retrieved from the JMX server. Multiple libraries can be entered separated by a semicolon.</p> <p>By default, the JMX monitor uses existing thread pools to bring information (counter names and values) from the JMX server (regular mode). However, if an additional classpath is specified, the default is the sandbox mode which uses additional threads taken from thread pool. To enable the monitor to use a separate thread pool (sandbox mode) even when not using additional classpath, set <code>_disableExtraClassPathExecutor</code> to <code>=false</code> in the <b>&lt;SiteScope root directory&gt;\groups\master.config</b> file. For details, see <a href="#">"Thread Pool Settings" on page 326</a>.</p> <p><b>Note:</b> When monitoring a WebLogic Application Server 11g (10.3.1 - 10.3.5) or 12c, this field is mandatory, and the <b>wlfullclient.jar</b> must be used. For details on creating the <b>wlfullclient.jar</b>, refer to Using the WebLogic JarBuilder Tool (<a href="http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html">http://download.oracle.com/docs/cd/E12840_01/wls/docs103/client/jarbuilder.html</a>).</p>
<b>Load additional classpath first</b>	Loads the additional classpath libraries before loading all the existing classpath libraries. If no additional classpath libraries are found, the other classpaths folders are loaded.

UI Element	Description
<b>Counters</b>	Server performance counters to check with this monitor. Use the <b>Get Counters</b> button to select counters. When the server being monitored is a WebLogic 11g or 12c server, see <a href="#">"How to create a JMX Monitor for a WebLogic Server" on page 327</a> for further details.
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. The counters that you can monitor vary according to the target application.</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>
<p><b>Arithmetic Counters</b></p> <p><b>Note:</b> The Arithmetic Counters feature was deprecated and replaced by Calculated Metrics. If you created Arithmetic Counters in an earlier version of SiteScope and performed a SiteScope upgrade, you need to recreate the counters in the Calculated Metrics panel, and then delete the Arithmetic Counters. For details on calculated metrics, see Calculated Metrics Settings in the Using SiteScope Guide. HPE plans to remove the Arithmetic Counters section from the JMX Monitor Settings in the next version of SiteScope.</p>	
	<b>Add Arithmetic Counter.</b> (Deprecated - no longer available)
	<b>Delete Arithmetic Counter.</b> Deletes the selected arithmetic counter from the Arithmetic Counters table.
<b>Original Counters</b>	The path and name of the original counter on which the arithmetic counter is calculated.
<b>Operator</b>	The operator (Rate) that is performed on the counter. The value in this column is not editable.
<b>Value</b>	This column is blank, and is not editable for the Rate operator.
<b>Arithmetic Counter Name</b>	The name of the arithmetic counter. This is the name of the on original counter on which the arithmetic counter is calculated with "Rate on" prefix. The value in this column is not editable.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section includes:


- ["General Notes/Tips" on the next page](#)
- ["Troubleshooting and Limitations" on the next page](#)

## General Notes/Tips

- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- The maximum number of counters that you can select for the JMX monitor 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.
- The JMX over RMI protocol is not firewall friendly.
- The Arithmetic Counters feature was deprecated and replaced by Calculated Metrics. For details about calculated metrics, see Calculated Metrics Settings in the Using SiteScope Guide. HPE plans to remove the Arithmetic Counters section from the JMX Monitor Settings in the next version of SiteScope.

## Troubleshooting and Limitations

- If you encounter "UnknownHostException" and the host does not match the one provided in the **JMX URL** box when monitoring a JBoss server, it is possible that the RMI codebase server name is set incorrectly. You should set the following java option in the JBoss configuration (for instance, using "run.config" in JBoss 5):  

```
-Djava.rmi.server.hostname="<FQDN>"
```
- SiteScope versions running on Java 1.6 or later do not support JMX monitoring of WebLogic 9.x because it runs on Java 1.5. For more details, see "RMI/IIOP SDK Error" in the Oracle documentation ([http://docs.oracle.com/cd/A97688\\_16/unix.903/relnotes/oc4j.htm](http://docs.oracle.com/cd/A97688_16/unix.903/relnotes/oc4j.htm)).
- 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 platforms, 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 in the SiteScope Dashboard.

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**.

# Chapter 44: KVM Monitor

The KVM monitor provides a solution for monitoring Kernel-based Virtual Machines (KVM) on Linux x86 and x86\_64 hardware that contains virtualization extensions. You can monitor multiple parameters or counters with a single monitor instance. This enables you to watch key operational factors that can seriously affect availability and degrade performance. Create a separate monitor instance for each server you are running.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the KVM monitor.

## Learn About

This section includes:

- ["KVM Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["License Consumption" below](#)

### KVM Monitor Overview

KVM is a virtualization technology that allows you to run multiple operating systems, including multiple instances of the same operating system, concurrently on the same physical computer.

SiteScope simplifies the monitoring of virtual infrastructure changes in dynamic, virtualized environments by automatically changing the SiteScope configuration according to changes in the virtual environment. KVM monitors are dynamically updated over time by adding or removing counters as virtual machines are added or removed. This enables you to configure the monitor one time, and leave it to automatically discover changes in the environment and update itself.

During initial monitor creation, the monitor uses the connection URI configured to access the VM 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.

You can also define the required thresholds for the counter's pattern. In this way, thresholds are also updated automatically when the counters are updated.

For more details on the dynamic monitoring mechanism, see Dynamic Monitoring Mechanism in the Using SiteScope Guide.

### Supported Platforms/Versions

This monitor supports monitoring remote servers running on UNIX remotes only. It has been tested on Linux #29-Ubuntu SMP 3.0.0-16-generic.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per host and one point per guest	One OSi license per monitored host


# Tasks

## How to Configure the KVM Monitor

### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- The monitored VM server must be directly accessible by the SiteScope server (no proxy involved).
- The Virsh and Virt-top command-line tools should be installed on the system. For details, see:
  - <https://help.ubuntu.com/community/KVM/Virsh>.
  - <http://linux.die.net/man/1/virt-top>
  - <http://people.redhat.com/~rjones/virt-top/>

### 2. Configure the monitor properties

- a. Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **KVM**. The New KVM Monitor dialog box opens.
- b. In the General Settings panel, enter a name and description for the monitor.
- c. In the KVM Monitor Settings panel, select the VM server you want to monitor (or add a new server) and specify the driver to which you want to connect in the **Connection URI** box. For user interface details, see the UI Descriptions section below.
- d. Click the **Get Counter** button, and select the counters you want to monitor from the Select Counters Form. The counters are added to the Preview tree in the **Patterns & Counters** section.
- e. For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
  - Clicking the **Add New Counter**  button to add an empty line to the table, and creating a pattern format using a regular expression.

#### Tip:

- (1). The pattern should always start and end with the forward slash ("/") character.
- (2). The "[" and "]" characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character).
- (3). Use "." to describe any character any number of times.


For example, `./*/Domains Information./*/Used Memory/` displays Used Memory counter for all VMs.

- Selecting a static counter, and editing the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.

**Note:** For details on the maximum number of counters that can be selected from the browsable tree and the maximum number of counters that can match the selected counter patterns when creating and updating dynamic monitors, see ["Maximum Number of Counters That Can be Saved" on page 341](#). If the maximum number of counters that can be deployed is exceeded, an error is written to the **RunMonitor.log**.

**Example:**

If you enter the pattern `./*/Domains Information/./*/Used Memory/`, the monitor retrieves the Used Memory counter for all VMs.

- f. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counter Preview tree.
- g. Set the frequency for updating counters from the server in the **Frequency of updating counters from server** box. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- h. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful for keeping track of the counters that were previously being monitored.
- i. Click **Verify & Save** or **Save** to save your settings.
- j. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

### 3. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the VM server and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:

- The **SiteScope Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.




For additional troubleshooting suggestions, see ["Tips/Troubleshooting" on page 341](#).



# UI Descriptions

## KVM Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of the VM server that you want to monitor. Select a server from the server list (only those UNIX remote servers that have been configured in SiteScope are displayed), or click the <b>Add Remote Server</b> to add a new UNIX server.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>When configuring this monitor on SiteScopes running on UNIX versions, only remote servers that have been configured with an <b>SSH</b> connection method are displayed. For details, see How to Configure Remote Windows Servers for SSH monitoring.</li> <li>When working in template mode, 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> </ul>
<b>Server to get measurements from</b>	(Available in template mode only) Name of any SiteScope remote server from which you want to get counters.
<b>Add Remote Server</b>	Opens the Add UNIX Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.
<b>Connection URI</b>	<p>URI of the driver of the VM server that you want to monitor.</p> <p><b>Default value:</b> qemu:///system</p>
<b>Patterns &amp; Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Click the <b>Add New Counter</b>  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the <b>Delete Counter</b>  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the <b>View Matches for Selected Pattern</b>  button to display counters that match the selected patterns.</p> <p><b>Note:</b> SiteScope uses Perl regular expressions for pattern matching.</p>

UI Element	Description
<b>Get Counters</b>	<p>Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.</p> <p>For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</p>
<b>Counter Preview</b>	<p>Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.</p>
<b>Frequency of updating counters from server</b>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p><b>Default value:</b> 15 minutes</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The update frequency cannot be less than the monitor run frequency in Monitor Run Settings.</li> <li>• When configuring this setting in a template, the variable value can only be in time units of seconds.</li> <li>• Static counters are never deleted.</li> </ul>
<b>Continue displaying counters that no longer exist after update</b>	<p>When selected, counters that no longer exist after running the update mechanism to retrieve counters from the monitored server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful, for example, if a disk fails or for keeping track of counters that were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings on the next update.</p> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b> This option is relevant for dynamic counters only (those set using a regular expression). Static counters that are no longer available are still displayed even when this check box is cleared.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

### KVM Host Information

Virsh Management/Node Information/Core(s) per socket  
Virsh Management/Node Information/CPU(s)  
Virsh Management/Node Information/CPU frequency  
Virsh Management/Node Information/CPU model  
Virsh Management/Node Information/CPU socket(s)  
Virsh Management/Node Information/Memory size  
Virsh Management/Node Information/NUMA cell(s)  
Virsh Management/Node Information/Thread(s) per core

### KVM virtual machines information

Virsh Management/Domains Information/vm1/Autostart  
Virsh Management/Domains Information/vm1/CPU(s)  
Virsh Management/Domains Information/vm1/CPU time  
Virsh Management/Domains Information/vm1/Id  
Virsh Management/Domains Information/vm1/Max memory  
Virsh Management/Domains Information/vm1/Name  
Virsh Management/Domains Information/vm1/OS Type  
Virsh Management/Domains Information/vm1/Persistent  
Virsh Management/Domains Information/vm1/Security DOI  
Virsh Management/Domains Information/vm1/Security label  
Virsh Management/Domains Information/vm1/Security model  
Virsh Management/Domains Information/vm1/State  
Virsh Management/Domains Information/vm1/Used memory  
Virsh Management/Domains Information/vm1/UUID  
Virsh Management/Domains Information/vm2/Autostart  
Virsh Management/Domains Information/vm2/CPU(s)  
Virsh Management/Domains Information/vm2/Id  
Virsh Management/Domains Information/vm2/Max memory  
Virsh Management/Domains Information/vm2/Name  
Virsh Management/Domains Information/vm2/OS Type  
Virsh Management/Domains Information/vm2/Persistent  
Virsh Management/Domains Information/vm2/Security DOI  
Virsh Management/Domains Information/vm2/Security model  
Virsh Management/Domains Information/vm2/State  
Virsh Management/Domains Information/vm2/Used memory  
Virsh Management/Domains Information/vm2/UUID

### KVM Domains Statistics Information

KVM Statistics/Domains/kvm\_ack\_irq  
KVM Statistics/Domains/kvm\_age\_page  
KVM Statistics/Domains/kvm\_apic  
KVM Statistics/Domains/kvm\_apic\_accept\_irq

KVM Statistics/Domains/kvm\_fpu  
KVM Statistics/Domains/kvm\_hv\_hypercall  
KVM Statistics/Domains/kvm\_hypercall  
KVM Statistics/Domains/kvm\_inj\_exception  
KVM Statistics/Domains/kvm\_inj\_virq  
KVM Statistics/Domains/kvm\_invlpga  
KVM Statistics/Domains/kvm\_ioapic\_set\_irq  
KVM Statistics/Domains/kvm\_mmio  
KVM Statistics/Domains/kvm\_msi\_set\_irq  
KVM Statistics/Domains/kvm\_msr  
KVM Statistics/Domains/kvm\_nested\_intercepts  
KVM Statistics/Domains/kvm\_nested\_intr\_vmexit  
KVM Statistics/Domains/kvm\_nested\_vmexit  
KVM Statistics/Domains/kvm\_nested\_vmexit\_inject  
KVM Statistics/Domains/kvm\_nested\_vmrunk  
KVM Statistics/Domains/kvm\_page\_fault  
KVM Statistics/Domains/kvm\_pic\_set\_irq  
KVM Statistics/Domains/kvm\_pio  
KVM Statistics/Domains/kvm\_set\_irq  
KVM Statistics/Domains/kvm\_skinit  
KVM Statistics/Domains/kvm\_try\_async\_get\_page  
KVM Statistics/Domains/kvm\_userspace\_exit  
KVM Statistics/Node/kvm\_ack\_irq  
KVM Statistics/Node/kvm\_age\_page  
KVM Statistics/Node/kvm\_apic  
KVM Statistics/Node/kvm\_apic\_accept\_irq  
KVM Statistics/Node/kvm\_apic\_ipi  
KVM Statistics/Node/kvm\_async\_pf\_completed  
KVM Statistics/Node/kvm\_async\_pf\_doublefault  
KVM Statistics/Node/kvm\_async\_pf\_not\_present  
KVM Statistics/Node/kvm\_async\_pf\_ready  
KVM Statistics/Node/kvm\_cpuid  
KVM Statistics/Node/kvm\_cr  
KVM Statistics/Node/kvm\_emulate\_insn  
KVM Statistics/Node/kvm\_entry  
KVM Statistics/Node/kvm\_exit  
KVM Statistics/Node/kvm\_exit(APIC\_ACCESS)  
KVM Statistics/Node/kvm\_exit(CPUID)  
KVM Statistics/Node/kvm\_exit(CR\_ACCESS)  
KVM Statistics/Node/kvm\_exit(DR\_ACCESS)  
KVM Statistics/Node/kvm\_exit(EPT\_MISCONFIG)  
KVM Statistics/Node/kvm\_exit(EPT\_VIOLATION)  
KVM Statistics/Node/kvm\_exit(EXCEPTION\_NMI)  
KVM Statistics/Node/kvm\_exit(EXTERNAL\_INTERRUPT)  
KVM Statistics/Node/kvm\_exit(HLT)  
KVM Statistics/Node/kvm\_exit(INVALID\_STATE)  
KVM Statistics/Node/kvm\_exit(INVLPGA)  
KVM Statistics/Node/kvm\_exit(IO\_INSTRUCTION)  
KVM Statistics/Node/kvm\_exit(MCE\_DURING\_VMENTRY)

<p>KVM Statistics/Domains/kvm_apic_ipi</p> <p>KVM Statistics/Domains/kvm_async_pf_completed</p> <p>KVM Statistics/Domains/kvm_async_pf_doublefault</p> <p>KVM Statistics/Domains/kvm_async_pf_not_present</p> <p>KVM Statistics/Domains/kvm_async_pf_ready</p> <p>KVM Statistics/Domains/kvm_cpuid</p> <p>KVM Statistics/Domains/kvm_cr</p> <p>KVM Statistics/Domains/kvm_emulate_insn</p> <p>KVM Statistics/Domains/kvm_entry</p> <p>KVM Statistics/Domains/kvm_exit</p> <p>KVM Statistics/Domains/kvm_exit(APIC_ACCESS)</p> <p>KVM Statistics/Domains/kvm_exit(CPUID)</p> <p>KVM Statistics/Domains/kvm_exit(CR_ACCESS)</p> <p>KVM Statistics/Domains/kvm_exit(DR_ACCESS)</p> <p>KVM Statistics/Domains/kvm_exit(EPT_MISCONFIG)</p> <p>KVM Statistics/Domains/kvm_exit(EPT_VIOLATION)</p> <p>KVM Statistics/Domains/kvm_exit(EXCEPTION_NMI)</p> <p>KVM Statistics/Domains/kvm_exit(EXTERNAL_INTERRUPT)</p> <p>KVM Statistics/Domains/kvm_exit(HLT)</p> <p>KVM Statistics/Domains/kvm_exit(INVALID_STATE)</p> <p>KVM Statistics/Domains/kvm_exit(INVLPG)</p> <p>KVM Statistics/Domains/kvm_exit(IO_INSTRUCTION)</p> <p>KVM Statistics/Domains/kvm_exit(MCE_DURING_VMENTRY)</p> <p>KVM Statistics/Domains/kvm_exit(MONITOR_INSTRUCTION)</p> <p>KVM Statistics/Domains/kvm_exit(MSR_READ)</p> <p>KVM Statistics/Domains/kvm_exit(MSR_WRITE)</p> <p>KVM Statistics/Domains/kvm_exit(MWAIT_INSTRUCTION)</p> <p>KVM Statistics/Domains/kvm_exit(NMI_WINDOW)</p> <p>KVM Statistics/Domains/kvm_exit(PAUSE_INSTRUCTION)</p> <p>KVM Statistics/Domains/kvm_exit(PENDING_INTERRUPT)</p> <p>KVM Statistics/Domains/kvm_exit(RDPMC)</p> <p>KVM Statistics/Domains/kvm_exit(RDTSC)</p> <p>KVM Statistics/Domains/kvm_exit(TASK_SWITCH)</p> <p>KVM Statistics/Domains/kvm_exit(TPR_BELOW_THRESHOLD)</p> <p>KVM Statistics/Domains/kvm_exit(TRIPLE_FAULT)</p> <p>KVM Statistics/Domains/kvm_exit(VMCALL)</p> <p>KVM Statistics/Domains/kvm_exit(VMCLEAR)</p> <p>KVM Statistics/Domains/kvm_exit(VMLAUNCH)</p> <p>KVM Statistics/Domains/kvm_exit(VMOFF)</p> <p>KVM Statistics/Domains/kvm_exit(VMON)</p> <p>KVM Statistics/Domains/kvm_exit(VMPTRLD)</p> <p>KVM Statistics/Domains/kvm_exit(VMPTRST)</p> <p>KVM Statistics/Domains/kvm_exit(VMREAD)</p> <p>KVM Statistics/Domains/kvm_exit(VMRESUME)</p> <p>KVM Statistics/Domains/kvm_exit(VMWRITE)</p> <p>KVM Statistics/Domains/kvm_exit(WBINVD)</p> <p>KVM Statistics/Domains/kvm_exit(XSETBV)</p>	<p>KVM Statistics/Node/kvm_exit(MONITOR_INSTRUCTION)</p> <p>KVM Statistics/Node/kvm_exit(MSR_READ)</p> <p>KVM Statistics/Node/kvm_exit(MSR_WRITE)</p> <p>KVM Statistics/Node/kvm_exit(MWAIT_INSTRUCTION)</p> <p>KVM Statistics/Node/kvm_exit(NMI_WINDOW)</p> <p>KVM Statistics/Node/kvm_exit(PAUSE_INSTRUCTION)</p> <p>KVM Statistics/Node/kvm_exit(PENDING_INTERRUPT)</p> <p>KVM Statistics/Node/kvm_exit(RDPMC)</p> <p>KVM Statistics/Node/kvm_exit(RDTSC)</p> <p>KVM Statistics/Node/kvm_exit(TASK_SWITCH)</p> <p>KVM Statistics/Node/kvm_exit(TPR_BELOW_THRESHOLD)</p> <p>KVM Statistics/Node/kvm_exit(TRIPLE_FAULT)</p> <p>KVM Statistics/Node/kvm_exit(VMCALL)</p> <p>KVM Statistics/Node/kvm_exit(VMCLEAR)</p> <p>KVM Statistics/Node/kvm_exit(VMLAUNCH)</p> <p>KVM Statistics/Node/kvm_exit(VMOFF)</p> <p>KVM Statistics/Node/kvm_exit(VMON)</p> <p>KVM Statistics/Node/kvm_exit(VMPTRLD)</p> <p>KVM Statistics/Node/kvm_exit(VMPTRST)</p> <p>KVM Statistics/Node/kvm_exit(VMREAD)</p> <p>KVM Statistics/Node/kvm_exit(VMRESUME)</p> <p>KVM Statistics/Node/kvm_exit(VMWRITE)</p> <p>KVM Statistics/Node/kvm_exit(WBINVD)</p> <p>KVM Statistics/Node/kvm_exit(XSETBV)</p> <p>KVM Statistics/Node/kvm_fpu</p> <p>KVM Statistics/Node/kvm_hv_hypercall</p> <p>KVM Statistics/Node/kvm_hypercall</p> <p>KVM Statistics/Node/kvm_inj_exception</p> <p>KVM Statistics/Node/kvm_inj_virq</p> <p>KVM Statistics/Node/kvm_invlpga</p> <p>KVM Statistics/Node/kvm_ioapic_set_irq</p> <p>KVM Statistics/Node/kvm_mmio</p> <p>KVM Statistics/Node/kvm_msi_set_irq</p> <p>KVM Statistics/Node/kvm_msr</p> <p>KVM Statistics/Node/kvm_nested_intercepts</p> <p>KVM Statistics/Node/kvm_nested_intr_vmexit</p> <p>KVM Statistics/Node/kvm_nested_vmexit</p> <p>KVM Statistics/Node/kvm_nested_vmexit_inject</p> <p>KVM Statistics/Node/kvm_nested_vmrunk</p> <p>KVM Statistics/Node/kvm_page_fault</p> <p>KVM Statistics/Node/kvm_pic_set_irq</p> <p>KVM Statistics/Node/kvm_pio</p> <p>KVM Statistics/Node/kvm_set_irq</p> <p>KVM Statistics/Node/kvm_skinit</p> <p>KVM Statistics/Node/kvm_try_async_get_page</p> <p>KVM Statistics/Node/kvm_userspace_exit</p>
---	---

## Tips/Troubleshooting

This section includes:

- ["General Notes" below](#)
- ["Maximum Number of Counters That Can be Saved" below](#)
- ["Troubleshooting Logs" below](#)

### General Notes

- When configuring this monitor in template mode, the **Add Remote Server** button is not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- This monitor supports setting fractional thresholds which are more useful than setting whole number thresholds when monitoring large disks (such as 1 terabyte and larger).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).

### Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the **\_browsableContentMaxCounters** parameter in the **master.config** file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the **\_maxCountersForRegexMatch** parameter in the **master.config** file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The **\_maxCountersForRegexMatch** parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both **\_browsableContentMaxCounters** and **\_maxCountersForRegexMatch** parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

### Troubleshooting Logs

1. Check for dynamic framework errors in:
  - **<SiteScope root directory>\logs\dynamic\_monitoring\_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.

- **<SiteScope root directory>\logs\dynamic\_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).

To check for dynamic monitoring errors, copy the following section from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####  
# Dynamic Monitoring  
#####  
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=  
DEBUG, dynamic.monitoring.appender  
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=false  
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG, dynamic.monitoring.appender  
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false  
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFileAppender  
log4j.appender.dynamic.monitoring.appender.File=../${log.file.path}/dynamic_monitoring.log  
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB  
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5  
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.PatternLayout  
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
```

2. Check for KVM monitor errors in:

**<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.

# Chapter 45: LDAP Monitor

This monitor enables you to verify 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the LDAP monitor.

## Learn About

This section includes:

- ["LDAP Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Status" below](#)
- ["License Consumption" on the next page](#)

### 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, monitor each of the servers. You may also want to monitor round trip time of the authentication process.

LDAP traffic is transmitted unsecured by default. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL) and installing a properly formatted certificate.

### Supported Platforms/Versions

This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.

### Status

Each time the LDAP monitor runs, it returns a status based on the time it takes to perform the connection. An error status or warning status is returned if the current value of the monitor is anything other than good. Errors occur if SiteScope is unable to connect, receives an unknown host name error, or the IP address does not match the host name.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitored host

## Tasks

### How to Configure the LDAP Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Tip:** The **LDAP Authentication Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see LDAP Authentication Status Tool in the Using SiteScope Guide.

## UI Descriptions

### LDAP Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Authentication Settings</b>	
<b>LDAP service provider</b>	<p>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.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"><li>• By default, LDAP version 2 is used. To use LDAP version 3, type <b>[LDAP-3]</b> before the URL.</li><li>• To enable LDAP over SSL, type <b>[LDAP-SSL]</b> before the URL.</li></ul>



UI Element	Description
<b>Security principal</b>	<p>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.</p> <p><b>Example:</b> uid=testuser,ou=TEST,o=mydomain.com</p> <p><b>Note:</b> To prevent binary data appearing in the output of LDAP queries, all binary attributes should be listed in the <b>LDAP binary attributes</b> field in <b>Preferences &gt; Infrastructure Preferences &gt; General Settings</b>.</p>
<b>Security credential</b>	<p>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 Settings</b>	
<b>Content match</b>	<p>Text string 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 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 Perl regular expression.</p> <p><b>Example:</b> /Temperature: (\d+). 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>
<b>Object query</b>	<p>An object query to look at an 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>For more information on LDAP queries, see <a href="http://technet.microsoft.com/es-es/library/aa996205(EXCHG.65).aspx">http://technet.microsoft.com/es-es/library/aa996205(EXCHG.65).aspx</a>.</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>

UI Element	Description
<b>LDAP filter</b>	<p>Performs an LDAP 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://download.oracle.com/javase/jndi/tutorial/basics/directory/filter.html">http://download.oracle.com/javase/jndi/tutorial/basics/directory/filter.html</a>.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- Retrieve first entry(s)
- Simple Query
- False Query
- Advanced Query
- Authentication
- Content verification

## Tips/Troubleshooting

### General Tips/Limitations

The monitor run summary string is limited to 100 characters. If the LDAP response is larger than the default value, you can increase this limit by adding the property `_ldapMaxSummary=<# of symbols in summary>` to the `<SiteScope root>\groups\master.config` file, and then restart SiteScope.

# Chapter 46: Link Check Monitor

This monitor 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Link Check monitor.

## Learn About

### 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.

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 want to check only a portion of your site without checking the entire site, then you can limit the search by specifying the exact URL that links to 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 need to run the link monitor only 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.

You can use the Link Check tool to export the result data from the last monitor run. To do this, you can select the "Use Monitor Run Result Data" from the properties tab of the monitor. If this option is not selected, the tool runs independently and displays all links and their status irrespective of the monitor configurations.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitored host

## Tasks

### How to Configure the Link Check Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor

as specified in Permissions and Credentials.

2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Tip:** The Link Check Tool is available when configuring this monitor to verify all the internal and external links on a Web page to ensure that they can be reached, and reports all links and their status. To use the tool when configuring or editing a monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions), click the **Use Tool** button. For details on the tool, see Link Check Tool.

## UI Descriptions

### Link Check Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>URL</b>	<p>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> <code>http://demo.thiscompany.com</code></p>
<b>Search external links</b>	<p>External links are links that have different host in comparison to that of the original base URL. The monitor follows 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>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>Amount of time, in seconds, that the monitor should wait for a page to begin 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>

UI Element	Description
<b>Maximum links</b>	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.  <b>Default value:</b> 800
<b>Maximum hops</b>	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.  <b>Default value:</b> Main page links  <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.
<b>POST data</b>	Form values required for the first page being checked. This is useful if you need to log on using an HTML form to reach the rest of the site that you are checking. Enter form values in the format <code>key=value</code> (one on each line).
<b>Authorization Settings</b>	
<b>Authorization user name</b>	User name to access the URL if required.
<b>Authorization password</b>	Password to access the URL if required.
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URL.
<b>Proxy server user name</b>	Proxy server user name if the proxy server requires a name to access the URL. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	Proxy server password if the proxy server requires a name to access the URL. Technical note: your proxy server must support Proxy-Authenticate for these options to function.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Chapter 47: Log File Monitor

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Log File monitor.

## Learn About

This section includes:

- ["Log File Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Customizing Log File Content Matches and Monitor Alerts" below](#)
- ["Support for IPv6 Addresses" on the next page](#)
- ["License Consumption" on the next page](#)

### 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 358](#).

### Supported Platforms/Versions

- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor also supports monitoring remote servers running on UNIX and HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see ["How to Configure the HP NonStop Resources Monitor" on page 307](#).

### 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 File 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 `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 *How to Configure an Alert* in the *Using SiteScope Guide*.

## Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the following protocols are supported:

- NetBIOS (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: `2004:DB8:2a:1005:230:48ff:fe73:982d`  
would be: `2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net`

For details on using IPv6, see *Support for IP Version 6* in the *Using SiteScope Guide*.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitored host

## Tasks

This section includes:

- ["How to Configure the Log File Monitor" on the next page](#)
- ["How to Use the Rules File" on the next page](#)

## How to Configure the Log File Monitor

### 1. Prerequisites

The following configuration requirements must be performed or verified before the Log File monitor can be used:

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- 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.
- For reading log files on remote Red Hat Linux machines, the **Disable connection caching** check box must be selected in the remote server's Advanced Settings, otherwise the Log File monitor will not work.

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

#### Note:

- 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.
- The **Regular Expression Tool** is available when configuring this monitor. For details on the tool, see Regular Expression Tool in the Using SiteScope Guide.

## How to Use the Rules File

In special cases, it may be necessary to create a custom rules file to specify different alerts for different log entry matches. When an application log message is read, this file is used to decide what action to take. An example rules file is located in **<SiteScope root directory>\examples\log\_monitor\sample.rules**.

### To use the sample.rules file:

1. Make a copy of the sample.rules file located in the **<SiteScope root directory>\examples\log\_monitor** directory, and rename it. There is no required naming convention.
2. Open the renamed file with an editor of your choice, and edit the file to meet your needs.

Each rule is a line of tab delimited fields in the format:

```
column<tab>match<tab>continue<tab>action<sp>actionParam1<sp>  
actionParam2<sp>...
```

where:



column is the column number (in ascending order starting from 0) of the log file to read, or ANY, or RULE to define a rule. Using ANY for the column checks the entire log message.

match is the text to match.

continue determines whether to continue searching the table.

action is the name of the alert action: SNMPTrap, Mailto, Page, Run, DatabaseAlert, Disable, NTLogEvent, SMS, Sound.

actionParameters are action specific parameters.

**Note:** Lines starting with "#" are ignored as comments.

#### Action descriptions:

Action	Parameters
SNMP	The first parameter is the beginning of the SNMP message (use "^" for spaces). The second parameter is the template file from the templates.snmp directory. The third parameter is the number of SNMP preferences or "default" (default SNMP preferences). This parameter must start with _id, and should be in the format: _id="preference_id"
Mailto	The first parameter is the address where the message is sent. The second parameter is the template file from the templates.mail directory.
Page	The first parameter is added to the beginning of the pager message (use "_" for spaces). The second parameter is the template file from the templates.page directory.
Run	The first parameter is the machine. If the script is to be run on a local machine, this parameter should be skipped. For a remote machine, the machine name should be prefixed with "remote:". The second parameter is the script file from the scripts directory. The third parameter is the template file from the <b>templates.script</b> directory. The fourth parameter is for the parameters. Use "_" as a separator between each parameter passed to a script. Use "#" before the property name to pass parameters from a monitor. You can use any property from the SiteScope Alert Template and Event Properties Directory. Note that "_" should be replaced with "#" when passed as a parameter to a script.
Using counters	Whenever linkCategory is set to a linkError, there is a linkErrorCount that counts the number of errors found. This is reset only when linkCategory is set to linkOk (when this occurs, linkOkCount starts counting matches).

- When you are finished, enter the full path to your rules file.

#### Examples:

Here are some examples for rules. Note that most of them use SNMP as the action, but you can define any other action in your rules file.

**Sample rule to forward trap if second column of log entry contains ERROR:**

```
2 ERROR n SNMPTrap error^in^column^two LogMessage _id="default"
```

**Sample rule to forward trap if any part of log entry contains ERROR:**

```
ANY ERROR n SNMPTrap error^in^log LogMessage _id="default"
```

**Sample rule to forward trap with default SNMP preferences(SNMPDefaultPreferences\_)**

```
ANY ERROR n SNMPTrap error^in^log LogMessage _id="default"
```

**Sample rule to forward trap and override default SNMP preferences by SNMPDefaultPreferences\_2**

```
ANY ERROR n SNMPTrap error^in^log LogMessage _id="2"
```

**Sample rule to send a pager message when first column contains DOWN:**

```
1 DOWN n Page help_help_help
```

**Sample rule to send email when first column contains DOWN:**

```
1 DOWN n Mailto sysadmin@this-company.com
```

**Sample rule to send two alerts when second column contains DEAD:**

```
2 DEAD y SNMPTrap app^is^dead LogMessage  
2 DEAD n Mailto sysadmin@this-company.com
```

**Sample default rule to always forward log messages as SNMP traps:**

```
ANY ANY n SNMPTrap default^rule LogMessage _id="default"
```

**Sample rule to run script when the log file contains ERROR:**

```
ANY Error n Run mailtest.bat
```

**Sample rule that runs a script with default template, and passes as parameters the value matching the regular expression between the () found in the log file and the log file name:**

```
ANY /(regularExp)/ y Run LogIt-LF.vbs Default <value>_<#logFile>
```

**Sample matching rules to set link category used by escalation:**

```
ANY LinkDowny SetCategory linkCategory linkError  
ANY LinkUp SetCategory linkCategory linkOk
```

**Sample escalation rules for link category:**

```
# first, send trap when problem happens the first time
RULE linkCategory y SNMPTrap first^alert LogMessage linkCategory = linkError and linkErrorCount
= 1

#

# second, after a minute send four traps
RULE linkCategory y SNMPTrap second^alert LogMessage linkCategory = linkError and
linkErrorTimeSinceFirst > 60 and linkErrorAlertCount < 4

#

# third, after five minutes, send five traps, at the rate of no more than one trap per minute
RULE linkCategory y SNMPTrap third^alert LogMessage linkCategory = linkError and
linkErrorTimeSinceFirst > 300 and linkErrorTimeSinceAlert > 60 and linkErrorAlertCount < 5

#

# send trap when problem is fixed
RULE linkCategory y SNMPTrap fourth^alert LogMessage linkCategory = linkOk and linkOkCount =
1

#

# run script when problem happens the first time
RULE linkCategory y Run mailtest.bat linkCategory = linkError and linkErrorCount = 1
```

**Sample rule to always send a trap:**

```
ANY ANY n SNMPTrap default^rule LogMessage
```

## UI Descriptions

### Log File Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	

UI Element	Description
<b>Server</b>	<p>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 Windows 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>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 (if the monitor does not work for one of these conditions, the other condition must be fulfilled, since both conditions do not always work on some machines). For details on how to configure a remote Windows server, see How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p> <p><b>Note:</b> For reading log files on remote Red Hat Linux machines, the <b>Disable connection caching</b> check box must be selected in the remote server's Advanced Settings, otherwise the Log File monitor will not work.</p>

UI Element	Description
<b>Log file path</b>	<p>Path to the log file you want to monitor.</p> <ul style="list-style-type: none"> <li>For reading log files on remote Windows 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 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 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 <a href="#">How to Configure SiteScope to Monitor a Remote Microsoft Windows Server</a> in the Using SiteScope Guide.</li> </ul> <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 <a href="#">SiteScope Date Variables and Examples for Log File Monitoring Policies</a> in the Using SiteScope Guide.</p>
<b>Run alerts</b>	<p>Method for running alerts for this monitor.</p> <ul style="list-style-type: none"> <li><b>For each log entry matched.</b> The monitor triggers alerts according to thresholds applied to each matching entry found. Since status can change according to thresholds for each matched entry, each alert action could be triggered many times within a monitor run. <b>Example:</b> If you want to send a warning alert on matched text value "power off" and an error alert if more than one server is turned off, set the following thresholds: <ul style="list-style-type: none"> <li>Error if matchCount &gt; 1</li> <li>Warning if value == 'power off'</li> </ul> <p>To send an error alert if only one threshold is matched, set Error if value == 'power off'.</p> <p>For details on how to create a Log File monitor that triggers customized alerts for content matches, see <a href="#">"Customizing Log File Content Matches and Monitor Alerts" on page 350</a>.</p> </li> <li><b>Once, after all log entries have been checked.</b> The monitor counts up the number of matches and then triggers alerts.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>The <b>For each log entry matched</b> method cannot work if a value greater than 1 is set as the alert setting trigger frequency in <b>Always, after the condition has occurred at least X times</b>.</li> </ul>

UI Element	Description
<b>Check from beginning</b>	<p>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>
<b>Content match</b>	<p>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.</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. The <code>/c</code> search modifier is not supported when Server-side processing is enabled. For details, see Regular Expressions Overview in the Using SiteScope Guide.</p> <p><b>Note:</b> When you create a report by clicking the monitor title, the report includes up to 10 values.</p>
<b>Open Tool</b>	<p>Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.</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 the 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>
<b>Rules file path</b>	<p>Enter the full path to your rules file. In special cases, it may be necessary to create a custom rules file to specify different alerts for different log entry matches. You can also set a parameter in the rules file to run script alerts. You can use any of the properties in the SiteScope Alert Template and Event Properties Directory in the Using SiteScope Guide.</p> <p>An example rules file is located in <b>&lt;SiteScope root directory&gt;\examples\log_monitor\sample.rules</b>. For instructions on how to use the file and example rules, see <a href="#">"How to Use the Rules File" on page 352</a>, or read the instructions in the file itself.</p>

UI Element	Description
<b>Match value labels</b>	<p>Use 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> When you create a report by clicking the monitor title, the report includes up to 10 match value labels.</p>
<b>Multi-line match</b>	<p>Runs a regular expression match on multiple lines of text.</p> <p><b>Default value:</b> Not selected</p>
<b>Server-side processing</b>	<p>Processes log file data on the remote 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>Use of this option is only recommended:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• For a log file that is frequently being written to between monitor runs. This way, all of the newly appended lines do not have to be copied across the network and parsed on the SiteScope server (the processing is done on the remote server and only the required lines would be copied across to SiteScope).</li> </ul> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• Server-side processing is enabled for remote Linux, Red Hat Enterprise Linux, and Oracle Solaris servers only. Windows SSH is not supported.</li> <li>• To enable server-side processing to work correctly when monitoring on a Solaris server, open the remote server settings for the monitored host (<b>Remote Servers &gt; UNIX Remote Servers &gt; Main Settings</b>), and enter a path to the bash interpreter in the <b>Initialize shell environment</b> field.</li> <li>• "Rule files" are not supported in this mode.</li> <li>• The /c search modifier is 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>Monitor remains 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>
<b>Timeout Settings</b>	

UI Element	Description
<b>Enable timeout</b>	If selected, the monitor stops its run after the specified timeout period has been exceeded. <b>Default value:</b> Not selected
<b>After timeout, resume reading from end of file</b>	If selected, the monitor resumes reading from the end of the log file during the next run, instead of from the current location. <b>Default value:</b> Selected <b>Note:</b> This setting is only available when <b>Enable timeout</b> is selected.
<b>Status after timeout</b>	The status condition that the monitor goes into if the monitor times out. The status categories include: Error, Warning, Good <b>Default value:</b> Warning <b>Note:</b> This setting is only available when <b>Enable timeout</b> is selected.
<b>Timeout (seconds)</b>	Amount of time, in seconds, that SiteScope should wait before the monitor times out. <b>Default value:</b> 60 seconds <b>Note:</b> This setting is only available when <b>Enable timeout</b> is selected.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

Alerts on matching text (for example, error messages)

- Lines
- lines/min
- matches
- matches/min
- value
- value2
- value3
- value4

## Tips/Troubleshooting

### General Tips/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When monitoring a log file on a FreeBSD remote server, make sure the correct path to the "cat" command is used in **<SiteScope root directory>\templates.os/FreeBSD.config**, since the command was moved



in the latest FreeBSD versions.

- If you use a single quote (') in a match command to retrieve log content and match keywords when using the **Server-side processing** option, you must replace the single quote with `\x27` or `'"'"'` (single quote, double quote, single quote, double quote, single quote), otherwise the single quote breaks the match command. Other special characters used in the regular expression should be escaped (in the usual way) if you want the characters to have their normal meaning. For more details, see Match String Literals.

# Chapter 48: Mail Monitor

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Mail monitor.

## Learn About

### 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.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitored host

## Tasks

### How to Configure the Mail Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Tip:** The **Mail Round Trip Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Mail Round Trip Tool in the Using SiteScope Guide.

# UI Descriptions

## Mail Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Action</b>	<p>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.</li></ul> <p><b>Note:</b> If this option is selected, the <b>Receive only content match</b> box must have a value to match against. Also, if this option is selected, 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 can retrieve the messages.</p> <ul style="list-style-type: none"><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>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>Mail address to which the test message should be sent.</p>
<b>Receiving protocol</b>	<p>Protocol used by the receiving mail server. Select one of the following options:</p> <ul style="list-style-type: none"><li>• <b>IMAP4</b> to use an IMAP4 mail server for receiving mail.</li><li>• <b>IMAP4S</b> to use a secure IMAP4 mail server for receiving mail.</li><li>• <b>POP3</b> to use a POP3 mail server for receiving mail.</li><li>• <b>POP3S</b> to use a secure POP3 mail server for receiving mail.</li></ul>
<b>Receiving email server</b>	<p>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>

UI Element	Description
<b>Receiving email server user name</b>	<p>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>
<b>Receiving email server password</b>	<p>Password, if necessary, for the receiving mail account.</p>
<b>Receive only content match</b>	<p>Text string 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><b>Note:</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>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. For example, /href=Doc\d+\.html/ or /href=doc\d+\.html/i.</li> <li>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, /Temperature: (\d+)/ would return the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold.</li> </ul>
<b>Attachment</b>	<p>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>
<b>Attachment encoding</b>	<p>The code page or encoding to use if the attachment file content uses an encoding that is different than the encoding used on server where SiteScope is running. 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>

UI Element	Description
<b>Timeout (seconds)</b>	<p>Amount of time, in 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>User name required for SMTP authentication if the SMTP server requires authentication before sending messages.</p>
<b>SMTP password</b>	<p>Password for the SMTP authentication (if required).</p>
<b>NTLM authentication</b>	<p>NTLM authentication version (1 or 2) if used by the email server.</p> <p><b>Default value:</b> none</p>
<b>SMTP SSL/TLS</b>	<p>Enables sending emails securely via SSL/TLS SMTP servers. When selected, the monitor sends all mails via SSL/TLS.</p> <p><b>Note:</b> By default, mail is sent via port 465 of the SMTP mail server unless you specify a different port in <b>Custom SMTP Port</b> (see below).</p> <p><b>Default value:</b> Not selected</p>
<b>Custom SMTP Port</b>	<p>Enables sending emails via a user-specified port. If this box is left empty, the default port for sending mail is used (465 for the SMTP mail server).</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- Round trip time – email delivery time
- Send time
- Receive time
- Status
- Content match on received email

# Chapter 49: MAPI Monitor

This monitor enables you to monitor the availability of Microsoft Exchange Server. 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the MAPI monitor.

## Learn About

This section includes:

- ["MAPI Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["License Consumption" below](#)

### 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 2007/2013, and for Outlook 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.

### Supported Platforms/Versions

This monitor is supported in SiteScopes that are running on Windows versions only.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitored host

## Tasks

This section includes:

- ["How to Prepare the System for Using the MAPI Monitor" on the next page](#)
- ["How to Configure the MAPI Monitor" on page 368](#)

## How to Prepare the System for Using the MAPI Monitor

**Note:** The following are 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).

### 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 panel 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.

## **How to Configure the MAPI Monitor**

1. Prerequisites

Before configuring the monitor, make sure the system is prepared for using the MAPI monitor as described in ["How to Prepare the System for Using the MAPI Monitor" on the previous page](#).

2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.



# UI Descriptions

## MAPI Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Receiver server</b>	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>	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>	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>	Windows account login name for the user associated with the above email account.
<b>Receiver password</b>	Windows account login password for the user name above.
<b>Sender server</b>	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>
<b>Sender mailbox</b>	Alias of the sending mailbox.
<b>Sender domain</b>	Domain to which both the sending mailbox owner and the sending Microsoft Exchange server belong.
<b>Sender user name</b>	Login name for the Windows account of the sending mailbox owner.
<b>Sender password</b>	Windows account login password for the sender account above.

UI Element	Description
<b>Transaction timeout (seconds)</b>	Amount of time, in 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>	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>	Email address of the SMTP sender.
<b>Receiver</b>	Email address of the receiver. This must match the <b>Receiver mailbox</b> alias specified above.
<b>Attachment</b>	Full path of a file to attach to the outgoing SMTP message.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Round Trip – email delivery time

**Note:** The **round trip time** counter is both measured and displayed in the SiteScope Dashboard in milliseconds; for all other monitors, it is measured in milliseconds and displayed in seconds.

# Chapter 50: Memcached Statistics Monitor

The Memcached Statistics monitor checks whether a memcached server is responding to a remote stats request, and stores the values returned in the response to a successful stats request.

Memcached is a high-performance, distributed memory object caching system, intended for use in speeding up dynamic web applications by alleviating database load. You can create a separate monitor instance for each Memcached server you are running. You may want to set up multiple monitors per server if several Memcached services were started on the different ports.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Memcached Statistics monitor.

## Learn About

### IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the TCP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSI license per monitored host

## Tasks

### How to Configure the Memcached Statistics Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Memcached Statistics Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Host</b>	Name of the Memcached server that you want to monitor.

UI Element	Description
<b>Port</b>	Port used by the Memcached Statistics server. <b>Default value:</b> 11211
<b>Timeout (milliseconds)</b>	Amount of time, in milliseconds, to wait for the connection to the port, and for any sending and receiving to complete. Once this time period passes, the Memcached Statistics monitor logs an error and reports an error status. <b>Default value:</b> 10000 milliseconds
<b>Counters</b>	Server statistics selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. <b>Note:</b> <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 (milliseconds) field 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>The total number of counters that can be monitored is limited to 100.</li> </ul> <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. You can configure the following counters for this monitor:
	<div> <b>Stats (number of connections, bytes in/out, etc):</b> <ul style="list-style-type: none"> <li>• pid</li> <li>• uptime</li> <li>• time</li> <li>• version</li> <li>• pointer_size</li> <li>• curr_items</li> <li>• total_items</li> <li>• bytes</li> <li>• curr_connections</li> <li>• total_connections</li> <li>• connection_structures</li> <li>• cmd_get</li> </ul> </div> <div> <ul style="list-style-type: none"> <li>• cmd_set</li> <li>• get_hits</li> <li>• get_misses</li> <li>• evictions</li> <li>• bytes_read</li> <li>• bytes_written</li> <li>• limit_maxbytes</li> <li>• threads</li> </ul> <b>stats slabs (Memory statistics):</b> <ul style="list-style-type: none"> <li>• active_slabs</li> <li>• total_malloced</li> </ul> </div>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Chapter 51: Memory Monitor

This monitor enables you to track how much physical and 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. Use this page to add a monitor or edit the monitor's properties.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Memory monitor.

## Learn About

This section includes:

- ["Memory Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)
- ["License Consumption" on the next page](#)

## 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 physical and virtual memory (which consists of both physical memory and swap memory) is currently in use on a server and how much space is free. Use the pages per second 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 SiteScope 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.

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH (see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide).
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.

**Note:** If you are monitoring a Windows remote server using the NetBIOS method, only virtual memory counters are available.

- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

**Note:** Physical memory (free space and used %) can only be monitored on Windows remote servers using the WMI connection method.

- Monitoring physical and virtual memory is not supported using the Rlogin connection method on UNIX remote servers.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor  Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

# Tasks

## How to Configure the Memory Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Tip:** The **Performance Counters Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor,

click the **Use Tool** button. For details on the tool, see Performance Counters Tool in the Using SiteScope Guide.

## UI Descriptions

### Memory Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>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> When working in template mode, 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>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

### Monitor Counters

Below is the list of counters that can be configured for this monitor:

- physical memory used %
- physical memory MB free
- virtual memory used % (previously percent used)
- virtual memory MB free (previously MB free)
- Pages/sec

## Tips/Troubleshooting

This section describes troubleshooting and limitations for the Memory monitor.

- ["General Notes/Tips" below](#)
- ["Troubleshooting and Limitations" below](#)

### General Notes/Tips

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- To get a detailed list of processes consuming most memory resources, create an Email alert using the **WithDiagnostics** template. When the monitor reaches the configured threshold, memory consumption for each process is sent in the body of the email alert.

### Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Memory monitor.

- ["Percentage of Virtual Memory Used Reaches 100%" below](#)
- ["Pages Per Second is Affecting System Performance" below](#)
- ["WMI Returns Incorrect Memory Values" on the next page](#)

#### Percentage of Virtual Memory Used Reaches 100%

**Problem:** The number of virtual memory used % reaches 100%, and services that are running may fail and new ones are unable to start. 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 in the Using SiteScope Guide.

**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 in the Using SiteScope Guide. For details on using the Service monitor, see ["Service Monitor" on page 589](#).

**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" on page 656](#).

#### 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.

#### **WMI Returns Incorrect Memory Values**

WMI returns incorrect values for the memory used % and MB free counters when the WMI connection method is used on a Windows Server 2008. This is due to an issue with WMI (not SiteScope).

#### **Monitor running on AIX remote servers does not monitor physical memory usage**

**Problem:** When the Memory monitor is configured to monitor a remote server running on an AIX operating system, the monitor does not monitor physical memory usage.

**Solution:** Make sure that the login account used for the remote connection has access to the `svmon` command.

# Chapter 52: Microsoft ASP Server Monitor

This monitor enables you to monitor the Active Server Pages (ASP) performance parameters on Windows systems. The error and warning thresholds for the monitor can be set on one or more ASP server performance statistics. 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft ASP Server monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" on the next page](#)

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

# Tasks

## How to Configure the Microsoft ASP Server Monitor

### 1. Prerequisites

- Make sure you have the specific access permissions required for this monitor as specified in Permissions and Credentials.
- The Microsoft ASP Server monitor makes use of performance counters to measure application server performance. SiteScopes running on Windows platforms need 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. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Microsoft ASP Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>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></p> <ul style="list-style-type: none"><li>• 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 in the Using SiteScope Guide.</li><li>• When working in template mode, 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></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 Serverslist 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Counters</b>	<p>Displays 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>

UI Element	Description
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a> .

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<ul style="list-style-type: none"><li>• Active Server Pages – Debugging Requests</li><li>• Active Server Pages – Errors During Script Runtime</li><li>• Active Server Pages – Errors From ASP Preprocessor</li><li>• Active Server Pages – Errors From Script Compilers</li><li>• Active Server Pages – Errors/Sec</li><li>• Active Server Pages – Request Bytes In Total</li><li>• Active Server Pages – Request Bytes Out Total</li><li>• Active Server Pages – Request Execution Time</li><li>• Active Server Pages – Request Wait Time</li><li>• Active Server Pages – Requests Disconnected</li><li>• Active Server Pages – Requests Executing</li><li>• Active Server Pages – Requests Failed Total</li><li>• Active Server Pages – Requests Not Authorized</li><li>• Active Server Pages – Requests Not Found</li><li>• Active Server Pages – Requests Queued</li><li>• Active Server Pages – Requests Rejected</li><li>• Active Server Pages – Requests Succeeded</li></ul>	<ul style="list-style-type: none"><li>• Active Server Pages – Requests Timed Out</li><li>• Active Server Pages – Requests Total</li><li>• Active Server Pages – Requests/Sec</li><li>• Active Server Pages – Script Engines Cached</li><li>• Active Server Pages – Session Duration</li><li>• Active Server Pages – Sessions Current</li><li>• Active Server Pages – Sessions Timed Out</li><li>• Active Server Pages – Sessions Total</li><li>• Active Server Pages – Template Cache Hit Rate</li><li>• Active Server Pages – Template Notifications</li><li>• Active Server Pages – Templates Cached</li><li>• Active Server Pages – Transactions Aborted</li><li>• Active Server Pages – Transactions Committed</li><li>• Active Server Pages – Transactions Pending</li><li>• Active Server Pages – Transactions Total</li><li>• Active Server Pages – Transactions/Sec</li></ul>
---	---

## Tips/Troubleshooting

### General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 53: Microsoft Exchange Monitor

This monitor enables you to monitor statistics of Microsoft Exchange Server on Windows platforms only.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of Microsoft Exchange Server monitoring. For details, see Microsoft Exchange Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Exchange monitor.

## Learn About

This section includes:

- ["Microsoft Exchange Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Setup Requirements" below](#)
- ["License Consumption" on page 385](#)

## Microsoft Exchange Monitor Overview

Use the Microsoft Exchange monitor to display important statistics about the messaging system handled by a Microsoft Exchange Server. 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 servers and objects.

By default, the Microsoft Exchange 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 Exchange Server 2007/2010. For details, see ["How to Prepare the System for Using the Microsoft Exchange Monitor" on page 385](#).

Create a separate Microsoft Exchange monitor instance for each Microsoft Exchange server in your environment. The Microsoft Exchange monitor is supported on Windows versions of SiteScope only.

## Supported Platforms/Versions

This monitor supports monitoring Microsoft Exchange Server 2007 with PowerShell v1.0, and Microsoft Exchange Server 2010 with PowerShell v2.0.

## Setup Requirements

- To configure Microsoft Exchange monitor, Exchange Management Shell must be installed on SiteScope server. Windows PowerShell 1.0 or 2.0 must be installed on the computer that runs the Exchange Management Shell.
- 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 "How to Prepare the System for Using the Microsoft Exchange Monitor" on the next page.

- To deploy the Microsoft Exchange solution template and run all monitors within it, your account must have permissions to run and receive output from the powershell commands below. For each cmdlet, the account you use must be delegated as follows (according to Microsoft Exchange Server 2007/2010, Permission Considerations section: <http://technet.microsoft.com/en-us/library/aa996881.aspx>):

cmdlet	Description
<b>Test-MAPIConnectivity</b>	<p>To run the Test-MapiConnectivity cmdlet, the account you use must be delegated the Exchange Server Administrators role and local Administrators group for the target server.</p> <p>To run the Test-MapiConnectivity cmdlet on a computer that has the Mailbox server role installed, you must log on by 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.</p>
<b>Test-ExchangeSearch</b>	<p>To run the Test-ExchangeSearch cmdlet, the account you use must be delegated the following:</p> <ul style="list-style-type: none"> <li>Exchange Recipient Administrator role</li> <li>Exchange Server Administrators role and local Administrators group for the target server</li> </ul>
<b>Test-MailFlow</b>	To run the Test-Mailflow cmdlet, the account you use must be delegated the Exchange Server Administrators role and local Administrators group for the server where the cmdlet is run.
<b>Test-OWAConnectivity</b>	To run the Test-OwaConnectivity cmdlet to test Outlook Web Access connectivity for all Exchange 2007/2010 virtual directories on a Client Access server, the account you use must be delegated the Exchange Server Administrators role and membership in the local Administrators group for the target server.
<b>Test-WebServicesConnectivity</b>	To run the Test-WebServicesConnectivity cmdlet, the account you use must be delegated the Exchange Administrator role and local Administrators group for the target server.

- To run each cmdlet, the server roles that correspond to the cmdlets you want to run must be installed on the Microsoft Exchange Server. When monitoring Microsoft Exchange Server 2007 or 2010, 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><b>Test-MAPIConnectivity</b></li> <li><b>Test-ExchangeSearch</b></li> </ul>



Server Role	Cmdlet
Hub Transport, Mailbox	<b>Test-MailFlow</b>
Client Access	<ul style="list-style-type: none"><li>• <b>Test-OWAConnectivity</b></li><li>• <b>Test-WebServicesConnectivity</b></li></ul>

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host  Note: This monitor is not available when using Community edition.

## Tasks

This section includes:

- ["How to Prepare the System for Using the Microsoft Exchange Monitor" below](#)
- ["How to Configure the Microsoft Exchange Monitor" on page 387](#)

### How to Prepare the System for Using the Microsoft Exchange Monitor

There are several important configuration requirements that must be performed or verified before the Microsoft Exchange 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.

Terminology	Description
Exchange Server Administrators	An account that has administrative privileges on the Exchange server.
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 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 and delegated the Exchange Server Administrators role (see definition above).

#### 1. **Create mailbox accounts on each Exchange Server to be monitored with the Microsoft Exchange monitor**

Exchange mailbox accounts are used by Microsoft Exchange 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 monitor.

You must configure a test mailbox in the Microsoft Exchange Server to retrieve health information for the Outlook Web Access and Web Services cmdlets.

- a. To configure a test mailbox in the Microsoft Exchange Server, run the script **New-TestCasConnectivityUser.ps1** in the Exchange Server to create a test mailbox. The script can be found under **<Exchange 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.

## 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 as to the Administrators group on the SiteScope server.

- a. Click **Start > Administrative Tools > Server Manager**.
- b. Expand the **Configuration > Local Users and Groups** folder in the left pane and click the **Groups** folder.
- c. Double-click the **Administrators** group icon to open the Administrators Properties window.
- d. Click the **Add** button to add each Mailbox Owner you expect to use with the Exchange 2007/2010 monitor.

## 3. Verify that the SiteScope user logon is a member of Administrators group or a domain administrator account and delegated the Exchange Server Administrators role

For more information about permissions, delegating roles, and the rights that are required for SiteScope user logon to monitor Microsoft Exchange Server 2007/2010, see ["Setup Requirements" on page 383](#).

**Caution:** The SiteScope user account must be a Local Administrator or a member of the domain admins group and delegated the Exchange Server Administrators role.

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.

## How to Configure the Microsoft Exchange Monitor

### 1. Prerequisites

Prepare the system for using the Microsoft Exchange monitor as described in ["How to Prepare the System for Using the Microsoft Exchange Monitor" on page 385](#).

There are several other key requirements for using this monitor. For details on this topic, see ["Setup Requirements" on page 383](#).

### 2. Enter the PowerShell execute command when using the Microsoft Exchange monitor on a 64-bit version of Windows 2003, 2008, or XP

To enable use of the Microsoft Exchange monitor on 64-bit version of Windows 2003, Windows 2008, or Windows XP (since a 32-bit application cannot access the system32 folder on a computer that is running a 64-bit version of Windows Server 2003, 2008, or of Windows XP), perform the following:

- a. Apply the Microsoft hotfix available from <http://support.microsoft.com/?scid=kb;en-us;942589>.
- b. In the **Power Shell execute command** box in **Preferences > Infrastructure Preferences > General Settings**, enter the PowerShell execute command. For example:  
`C:\Windows\Sysnative\WindowsPowerShell\v1.0\powershell.exe`

**Note:** Symlink Sysnative is not available by default on Windows 2003 or Windows XP.

### 3. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

### 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.

## UI Descriptions

### Microsoft Exchange Monitor Settings

User interface elements are described below:

UI Element	Description
Exchange server	Name of the server running Microsoft Exchange Server that you want to monitor.
Exchange domain	Domain name and the mailbox of the server running Microsoft Exchange Server that you want to monitor.

UI Element	Description
<b>Mailbox</b>	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>	<p>Full path to the Microsoft Exchange Server Management Shell console file.</p> <p><b>Example:</b></p> <ul style="list-style-type: none"> <li>On Microsoft Exchange 2007: <b>C:\Program Files\Microsoft\Exchange Server\Bin\ExShell.psc1</b></li> <li>On Microsoft Exchange 2010: <b>C:\Program Files\Microsoft\Exchange Server\V14\Bin\ExShell.psc1</b></li> </ul> <p><b>Note:</b> For Microsoft Exchange 2010, we recommend using the <b>RemoteExchange.psc1</b> file instead of <b>ExShell.psc1</b> (located in the same folder), especially if you encounter issues receiving counter values. When using <b>RemoteExchange.psc1</b>, we recommend setting a timeout value in the range of 3-5 minutes (180-300 seconds) instead of using the default timeout value of 120 seconds.</p>
<b>Timeout (seconds)</b>	<p>Amount of 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.</p> <p><b>Default value:</b> 120 seconds</p>
<b>Counters</b>	<p>Displays 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>UnitType.</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>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<ul style="list-style-type: none"> <li>• MAPI Connectivity/Result</li> <li>• MAPI Connectivity/Latency</li> <li>• Mail Flow/TestMailflowResult</li> <li>• Mail Flow/MessageLatencyTime</li> <li>• Exchange Search/ResultFound</li> <li>• Exchange Search/SearchTime (in Exchange 2007)</li> <li>• Exchange Search/SearchTimeInSeconds (in Exchange 2010)</li> <li>• OWA Connectivity/Result</li> <li>• OWA Connectivity/Latency</li> </ul>	<ul style="list-style-type: none"> <li>• Web Services Connectivity/CreateItem/Result</li> <li>• Web Services Connectivity/CreateItem/Latency</li> <li>• Web Services Connectivity/DeleteItem/Result</li> <li>• Web Services Connectivity/DeleteItem/Latency</li> <li>• Web Services Connectivity/GetFolder/Result</li> <li>• Web Services Connectivity/GetFolder/Latency</li> <li>• Web Services Connectivity/SyncFolderItems/Result</li> <li>• Web Services Connectivity/SyncFolderItems/Latency</li> </ul>
--	--

## Tips/Troubleshooting

### Unable to Connect to Microsoft Exchange Server 2010 and Receive Counters

If you are unable to connect to the Microsoft Exchange Server 2010 and receive counters, make sure you have the correct PowerShell startup parameters.

1. Open PowerShell and type the following to create a default PowerShell profile applicable to all users and automatically load the Exchange snap-in:
 

```
if (!(test-path $profile.AllUsersAllHosts)) {new-item -type file -path $profile.AllUsersAllHosts -force}
notepad $profile.AllUsersAllHosts
```
2. Add the following syntax to the **\$profile.AllUsersAllHosts** file:
 

```
. $env:ExchangeInstallPath\bin\RemoteExchange.ps1
Connect-ExchangeServer -auto
```
3. Save your changes and exit PowerShell.
4. Restart the SiteScope service.
5. Go into SiteScope and define the Microsoft Exchange monitor as described in the UI Descriptions section above.

# Chapter 54: Microsoft Exchange Base Monitor

This monitor enables you to monitor statistics of Microsoft Exchange Server 2010 and 2013 on Windows platforms only. This monitor provides monitoring for Client Access and Mailbox server roles, improved scalability, and an extended set of performance metrics from Microsoft Exchange Server 2013.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of Microsoft Exchange Server monitoring. For details, see Microsoft Exchange Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **Microsoft Exchange Base** monitor.

## Learn About

This section includes:

- ["Microsoft Exchange Base Monitor Overview" below](#)
- ["Supported Platforms/Versions" on the next page](#)
- ["Exchange Cmdlets Used by the Monitor" on the next page](#)
- ["License Consumption" on page 400](#)

## Microsoft Exchange Base Monitor Overview

Use the Microsoft Exchange Base monitor to display important statistics about the messaging system handled by a Microsoft Exchange 2010 or 2013 Server. 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 servers and objects.

The Microsoft Exchange Base monitor runs command-lets (cmdlets) to provide health information.

For Microsoft Exchange Server 2013, it can run the following cmdlets:

Cmdlets	Health Information
Get-StoreUsageStatistics	Store usage statistics data
Test-ActiveSyncConnectivity	Results of Exchange ActiveSync tests
Test-AssistantHealth	Mailbox Assistance performance data
Test-CalendarConnectivity	Results of anonymous calendar sharing tests
Test-ExchangeSearch	Results of Exchange search test
Test-ImapConnectivity	Results of IMAP4 service test

Cmdlets	Health Information
Test-Mailflow	Results of end to end mail delivery test
Test-MAPIConnectivity	Results of mailbox databases tests
Test-MRSHealth	Results of mailbox replication service test
Test-OutlookWebServices	Results of web services functionality tests
Test-PopConnectivity	Results of POP3 service test
Test-PowerShellConnectivity	Results of PowerShell remoting test
Test-ReplicationHealth	Results of DAG members tests
Test-ServiceHealth	Results of required services are running test
Test-WebServicesConnectivity	Results of web services functionality tests

For Microsoft Exchange Server 2010, it can run the following cmdlets:

Cmdlets	Health Information
Test-ExchangeSearch	Results of Exchange search test
Test-Mailflow	Results of end to end mail delivery test
Test-MAPIConnectivity	Results of mailbox databases tests
Test-OWAConnectivity	Results of Microsoft Office Outlook Web Access test
Test-WebServicesConnectivity	Results of web services functionality tests

Create a separate Microsoft Exchange Base monitor instance for each Microsoft Exchange server in your environment. The Microsoft Exchange Base monitor is supported on Windows versions of SiteScope only.

## Supported Platforms/Versions

Microsoft Exchange Server 2010 and 2013 on Windows platforms only.

**Note:** PowerShell v2.0 must be used on the SiteScope-side.

## Exchange Cmdlets Used by the Monitor

The following table includes a list of cmdlets that the monitor uses to gather information from the Exchange Server. To see what permissions you need in the Microsoft Exchange Server, refer to [Important: Update for Permissions in Exchange 2010](#) (for Microsoft Exchange Server 2010), or [http://technet.microsoft.com/en-us/library/dd638127\(v=exchg.150\).aspx](http://technet.microsoft.com/en-us/library/dd638127(v=exchg.150).aspx) (for Microsoft Exchange Server 2013).

cmdlets	Description
<b>Test-AssigmentHealth</b>	<p>Verifies that the Microsoft Exchange Mailbox Assistants service (MSEExchangeMailboxAssistants) is healthy, to recover from health issues, and to report the status of the diagnosis or recovery action.</p> <p>The Mailbox Assistants service runs on all servers that have the Mailbox server role installed. This service is responsible for scheduling and dispatching several assistants that ensure mailboxes function correctly.</p> <p>By default, when you run this cmdlet, it returns the RunspaceId, events, and performance counters in a table format.</p> <p>For details, see <a href="http://technet.microsoft.com/en-gb/library/ff829911(v=exchg.150).aspx">http://technet.microsoft.com/en-gb/library/ff829911(v=exchg.150).aspx</a>.</p> <p>This monitor collects Performance Counters only.</p>
<b>Get-StoreUsageStatistics</b>	<p>Aids in diagnosing performance issues with your servers or databases.</p> <p>The Microsoft Exchange Information Store service collects per-user information on latency, input/output (I/O), page counts, processor usage, and TimeInServer. The TimeInServer metric represents the total time that synchronous and asynchronous requests spend in the Microsoft Exchange Information Store service for a user's mailbox. You can retrieve this resource information in the Microsoft Exchange Information Store service for the 25 highest usage accounts on a specified database. Usage of a mailbox is defined as the amount of server time spent in performing operations for that mailbox. The cmdlet reports the top 25 users for every one-minute period for the last 10 minutes (250 objects per ten-minute interval). The resource usage is an indicator of the load that different users are placing on the server.</p> <p>For details, see <a href="http://technet.microsoft.com/en-gb/library/dd876852(v=exchg.150).aspx">http://technet.microsoft.com/en-gb/library/dd876852(v=exchg.150).aspx</a>.</p> <p>This monitor gets the arithmetic average of values for selected counters.</p>



cmdlets	Description
<b>Test-CalendarConnectivity</b>	<p>Verifies that anonymous calendar sharing is enabled and working properly. The Calendar virtual directory is a subdirectory of the Microsoft Office Outlook Web App virtual directory. When you run this command without any parameters, the command tests against all Outlook Web App calendar virtual directories.</p> <p>To test virtual directories on a Client Access server, there must be a test Active Directory account. There must also be a test mailbox in each Active Directory site that hosts mailboxes that can be accessed through the virtual directories being tested. You can create the test account by running the New-TestCasConnectivityUser.ps1 script. The default location for this file is: \\Program Files\Microsoft\Exchange Server\V15\Scripts.</p> <p>If the test environment wasn't created during the Mailbox server setup, you're prompted to run the script that creates the test mailboxes and test users when you run this command.</p> <p>If the server hosting the test mailbox isn't available, the command returns an error that might not clearly identify the problem. To avoid this, use the Test-MapiConnectivity cmdlet to verify that the server that hosts the test mailbox is running and that the mailbox is available before you run this command.</p> <p>For details, see <a href="http://technet.microsoft.com/en-gb/library/ff607308(v=exchg.150).aspx">http://technet.microsoft.com/en-gb/library/ff607308(v=exchg.150).aspx</a>.</p> <p>The TestType parameter specifies whether the command tests internal or external URLs. Values are Internal and External. If you don't specify this parameter, the default is TestType:Internal.</p> <p>This monitor uses Internal TestType.</p>
<b>Test-ExchangeSearch</b>	<p>Tests that Exchange Search is currently enabled and is indexing new email messages in a timely manner.</p> <p>This cmdlet creates a hidden message and an attachment visible only to Exchange Search. Unless a mailbox is specified in the Identity parameter, the hidden message is stored in the System Attendant mailbox. The command waits for the message to be indexed and then searches for the content. It reports success or failure depending on whether the message is found after the interval set in the IndexingTimeoutInSeconds parameter has elapsed.</p> <p>You can use the Verbose switch to get detailed information about each step performed by the cmdlet as part of the test.</p> <p>For details, see <a href="http://technet.microsoft.com/en-us/library/bb124733(v=exchg.150).aspx">http://technet.microsoft.com/en-us/library/bb124733(v=exchg.150).aspx</a>.</p> <p>The "Latency" counter is converted to seconds.</p>

cmdlets	Description
<b>Test-ImapConnectivity</b>	<p>Verifies that the IMAP4 service is running as expected. This cmdlet can be used to test the IMAP4 functionality for a specified Client Access server for all mailboxes on servers running Microsoft Exchange Server 2013 in the same Active Directory site.</p> <p>For details, see <a href="http://technet.microsoft.com/en-gb/library/bb738126(v=exchg.150).aspx">http://technet.microsoft.com/en-gb/library/bb738126(v=exchg.150).aspx</a>.</p> <p>The following parameters are used in the exchange command:</p> <ol style="list-style-type: none"> <li>1. LightMode parameter. This instructs the command to perform a test logon only to the server using the IMAP4 protocol. If you do not use this parameter, the test also checks the sending and receiving of a message using the IMAP4 protocol.</li> <li>2. PortClientAccessServer parameter. This specifies the port to use to connect to the Client Access server. The default port is 143 for Plain Text/TLS or 993 for SSL. The valid range is from 0 through 65,535.</li> </ol> <p>You can change the port in the <b>IMAP4 service port</b> field in the monitor settings.</p> <p>The "Latency" counter is converted to seconds.</p>
<b>Test-PopConnectivity</b>	<p>Use the Test-PopConnectivity cmdlet to verify that the POP3 service is running as expected. The Test-PopConnectivity cmdlet can be used to test the POP3 functionality for a specified Client Access server for all mailboxes on servers running Microsoft Exchange Server 2013 in the same Active Directory site.</p> <p>For details, see <a href="http://technet.microsoft.com/en-gb/library/bb738143(v=exchg.150).aspx">http://technet.microsoft.com/en-gb/library/bb738143(v=exchg.150).aspx</a>.</p> <p>The following parameters are used in the exchange command:</p> <ol style="list-style-type: none"> <li>1. LightMode parameter. This instructs the command to perform a test logon only to the server using the POP3 protocol. If you do not use this parameter, the test also checks the sending and receiving of a message using the POP3 protocol.</li> <li>2. PortClientAccessServer parameter. This specifies the port to use to connect to the Client Access server. The default port is 110 for Plain Text/TLS or 995 for SSL. The valid range is from 0 through 65,535.</li> </ol> <p>You can change the port in the <b>POP3 service port</b> field in the monitor settings.</p> <p>The "Latency" counter is converted to seconds.</p>

cmdlets	Description
<b>Test-PowerShellConnectivity</b>	<p>Tests whether Windows PowerShell remoting on the target Client Access server is functioning correctly.</p> <p>The Test-PowerShellConnectivity cmdlet connects to a Client Access server to test whether Windows PowerShell remoting on that server is working correctly and whether the Client Access server can perform commands against a remote Mailbox server.</p> <p>When you run this cmdlet, you must specify either the fully qualified domain name (FQDN) of the Client Access server to connect to by using the ClientAccessServer parameter, or the Uniform Resource Identifier (URI) of a Client Access server by using the ConnectionUri parameter. You can't use both the ClientAccessServer and ConnectionUri parameters in the same command.</p> <p>The first time you use the Test-PowerShellConnectivity cmdlet with the ClientAccessServer parameter, you might be required to create a test user. To create a test user, use the New-TestCasConnectivityUser.ps1 script.</p> <p>For details, see <a href="http://technet.microsoft.com/en-gb/library/dd335166(v=exchg.150).aspx">http://technet.microsoft.com/en-gb/library/dd335166(v=exchg.150).aspx</a>.</p> <p>This monitor uses the VirtualDirectoryName parameter in the exchange command . This parameter specifies the virtual directory on the Client Access server to test. The VirtualDirectoryName parameter can only be used with the ClientAccessServer parameter. If the VirtualDirectoryName parameter is not specified, all virtual directories on the Client Access server are tested.</p> <p>This monitor uses the “PowerShell (Default Web Site)” value by default. You can change this in the <b>PowerShell virtual directory name</b> field in the monitor settings.</p> <p>The “Latency” counter is converted to seconds.</p>
<b>Test-MRSHealth</b>	<p>Tests the health of an instance of the Microsoft Exchange Mailbox Replication service.</p> <p>The Microsoft Exchange Mailbox Replication service runs on Client Access servers. This command ensures that the Mailbox Replication service is running and that it responds to a remote procedure call (RPC) ping check.</p> <p>For details, see <a href="http://technet.microsoft.com/en-us/library/ee332325(v=exchg.150).aspx">http://technet.microsoft.com/en-us/library/ee332325(v=exchg.150).aspx</a>.</p> <p>This monitor uses “Passed” counters for different checks.</p>

cmdlets	Description
<b>Test-ReplicationHealth</b>	<p>Checks all aspects of replication and replay, and provides status for a specific Mailbox server in a database availability group (DAG).</p> <p>This cmdlet is designed for the proactive monitoring of continuous replication and the continuous replication pipeline, the availability of Active Manager, and the health and status of the underlying cluster service, quorum, and network components. The Test-ReplicationHealth cmdlet can be run locally or remotely against any Mailbox server in a DAG.</p> <p>For details, see <a href="http://technet.microsoft.com/en-gb/library/bb691314(v=exchg.150).aspx">http://technet.microsoft.com/en-gb/library/bb691314(v=exchg.150).aspx</a>.</p> <p>This monitor uses “Result” counters for different checks. Counters can have the following values: “Passed”, “*FAILED*”.</p>
<b>Test-ServiceHealth</b>	<p>Tests whether all the Microsoft Windows services that Exchange requires on a server have started. The cmdlet returns an error for any service required by a configured role when the service is set to start automatically and isn't currently running.</p> <p>For details, see <a href="http://technet.microsoft.com/en-gb/library/aa998852(v=exchg.150).aspx">http://technet.microsoft.com/en-gb/library/aa998852(v=exchg.150).aspx</a>.</p> <p>This monitor combines all “ServicesNotRunning” list values in a common list, as follows: {serviceName1, serviceName2, serviceName3}. An empty list is displayed as: {}</p>
<b>Test-WebServicesConnectivity</b>	<p>Performs basic operations to verify the functionality of Exchange Web Services on a server running Microsoft Exchange Server 2013.</p> <p>The cmdlet tests the functionality of Exchange Web Services, and performs basic operations to verify the functionality of Outlook Anywhere. The results of each test are returned by the Exchange Management Shell.</p> <p>For details, see <a href="http://technet.microsoft.com/en-us/library/aa998328(v=exchg.150).aspx">http://technet.microsoft.com/en-us/library/aa998328(v=exchg.150).aspx</a>.</p> <p>The “Latency” counter is converted to seconds.</p>

cmdlets	Description
<b>Test-MAPIConnectivity</b>	<p>Verifies server functionality by logging on to the mailbox that you specify (or to the SystemMailbox if you don't specify the Identity parameter) and retrieving a list of items in the Inbox. Logging on to the mailbox tests two critical protocols used when a client connects to a Mailbox server: MAPI and LDAP. During authentication, the cmdlet indirectly verifies that the MAPI server, Exchange store, and Directory Service Access (DSAccess) are working.</p> <p>The cmdlet logs on to the mailbox that you specify using the credentials of the account with which you are logged on to the local computer. After a successful authentication, the cmdlet accesses the mailbox to verify that the database is working. If a successful connection to a mailbox is made, the cmdlet also determines the time that the logon attempt occurred.</p> <p>There are three distinct parameters that you can use with the command:</p> <ul style="list-style-type: none"> <li>• Database. The Database parameter takes a database identity and tests the ability to log on to the system mailbox on the specified database.</li> <li>• Identity. The Identity parameter takes a mailbox identity and tests the ability to log on to a specific mailbox.</li> <li>• Server. The Server parameter takes a server identity and tests the ability to log on to each system mailbox on the specified server.</li> </ul> <p>For details, see <a href="http://technet.microsoft.com/en-us/library/bb123681(v=exchg.150).aspx">http://technet.microsoft.com/en-us/library/bb123681(v=exchg.150).aspx</a>.</p> <p>The “Latency” counter is an arithmetic average of “Latency” database counters, converted to seconds.</p> <p>The “Result” counter is a composite value, that might contain the following values: “Success”, “Failure”, or “Failure for Databases: database1, database2,...”</p>

cmdlets	Description
<b>Test-Mailflow</b>	<p>Diagnoses whether mail can be successfully sent from and delivered to the system mailbox on a Mailbox server. It also verifies that email is sent between Mailbox servers within a defined latency threshold.</p> <p>This cmdlet tests mail submission, transport, and delivery. The cmdlet verifies that each Mailbox server can successfully send itself a message. You can also use this cmdlet to verify that the system mailbox on one Mailbox server can successfully send a message to the system mailbox on another Mailbox server.</p> <p>If more than one of these parameters is specified, the <code>AutoDiscoverTargetMailboxServer</code> parameter takes precedence over the <code>TargetEmailAddress</code> and <code>TargetMailboxServer</code> parameters. The <code>TargetMailboxServer</code> parameter takes precedence over the <code>TargetEmailAddress</code> parameter. A system mailbox must be present on all servers involved in the test.</p> <p>For details, see <a href="http://technet.microsoft.com/en-us/library/aa995894(v=exchg.150).aspx">http://technet.microsoft.com/en-us/library/aa995894(v=exchg.150).aspx</a>.</p> <p>The “MessageLatencyTime” counter is converted to seconds.</p>
<b>Test-ActiveSyncConnectivity</b>	<p>Performs a full synchronization against a specified mailbox to test the configuration of Microsoft Exchange ActiveSync.</p> <p>For details, see <a href="http://technet.microsoft.com/en-us/library/bb123540(v=exchg.150).aspx">http://technet.microsoft.com/en-us/library/bb123540(v=exchg.150).aspx</a>.</p> <p>The “Latency” counters are converted to seconds.</p>
<b>Test-OutlookWebServices</b>	<p>Verifies the Autodiscover service settings for Microsoft Outlook on a computer running Microsoft Exchange Server 2010 that has the Client Access server role installed.</p> <p>The cmdlet uses a specified email address to verify that the Outlook provider is configured correctly.</p> <p>For details, see <a href="http://technet.microsoft.com/en-us/library/bb124509(v=exchg.141).aspx">http://technet.microsoft.com/en-us/library/bb124509(v=exchg.141).aspx</a>.</p> <p>The “Latency” counters are converted to seconds.</p>

cmdlets	Description
<p><b>Test-OWAConnectivity</b> (for Microsoft Exchange Server 2010 only)</p>	<p>Verifies that Microsoft Office Outlook Web App is running as expected. The Test-OwaConnectivity cmdlet can be used to test Outlook Web App connectivity for all Microsoft Exchange Server 2010 virtual directories on a specified Client Access server for all mailboxes on servers running Exchange that are in the same Active Directory site. The Test-OwaConnectivity cmdlet can also be used to test the connectivity for an individual Exchange Outlook Web App URL.</p> <p>To test all Exchange Outlook Web App virtual directories on a Client Access server, there must be a test Active Directory account. There must also be a test mailbox in each Active Directory site that hosts mailboxes that can be accessed through the virtual directories being tested. If the test environment wasn't created during the Mailbox server setup, you are prompted to run the script that creates the test mailboxes and test users when you run the Test-OwaConnectivity cmdlet.</p> <p>If the server that is hosting the test mailbox is not available, the Test-OWAConnectivity cmdlet will return an error that might not clearly identify the problem. To avoid this, check that the server that hosts the test mailbox is running and that the mailbox is available before you run the Test-OWAConnectivity cmdlet.</p> <p>If the server hosting the test mailbox isn't available, the Test-OwaConnectivity cmdlet returns an error that might not clearly identify the problem. To avoid this, check that the server that hosts the test mailbox is running and that the mailbox is available before you run the Test-OwaConnectivity cmdlet. You can use the Test-MapiConnectivity cmdlet to do this.</p> <p>If you run the Test-OwaConnectivity cmdlet on a Client Access server without using either the ClientAccessServer parameter or the URL parameter, the cmdlet tests the server on which you run the cmdlet. To test a specific Client Access server, use the ClientAccessServer parameter.</p> <p>To test a single URL, run the Test-OwaConnectivity cmdlet with the URL parameter and credentials for an existing Exchange mailbox. If the URL is behind a load balancer, you can't predict which Client Access server the command will test. Because credentials are required as part of the parameters when you use the URL parameter, you can use any account to run the Test-OwaConnectivity cmdlet when you use the URL parameter.</p> <p>If the command encounters a virtual directory that doesn't require Secure Sockets Layer (SSL), the command skips that directory unless the AllowUnsecureAccess parameter is used. If the AllowUnsecureAccess parameter is used, communications between servers are sent in clear text for purposes of the test.</p> <p>The Test-OwaConnectivity cmdlet can be run as a one-time interactive task or as a scheduled task under Microsoft System Center Operations Manager 2007 control. To run the Test-OwaConnectivity cmdlet as a System Center Operations Manager 2007 task, the Client Access test mailbox must be</p>

cmdlets	Description
	available on the Mailbox servers that the cmdlet tests against.  For details, see <a href="http://technet.microsoft.com/en-us/library/aa997682%28v=exchg.141%29.aspx">http://technet.microsoft.com/en-us/library/aa997682%28v=exchg.141%29.aspx</a> .

## License Consumption

Points-base Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host  Note: This monitor is not available when using Community Edition.

## Tasks

This section includes:

- "How to Prepare the System for Using the Microsoft Exchange Base Monitor" below
- "How to Configure the Microsoft Exchange Base Monitor" on the next page

### How to Prepare the System for Using the Microsoft Exchange Base Monitor

There are several important configuration requirements that must be performed or verified before the Microsoft Exchange Base 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.

Terminology	Description
Exchange Server Administrators	An account that has administrative privileges on the Exchange server.
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 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 and delegated the Exchange Server Administrators role (see definition above).

#### 1. Create mailbox accounts on each Exchange Server to be monitored with the Microsoft Exchange Base monitor

Exchange mailbox accounts are used by Microsoft Exchange Base 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 monitor.

You must configure a test mailbox in the Microsoft Exchange Server to retrieve health information for the Outlook Web Access, Web Services, Calendar, and PowerShell cmdlets.

- a. To configure a test mailbox in the Microsoft Exchange Server, run the script **New-TestCasConnectivityUser.ps1** in the Exchange Server to create a test mailbox. The script can be found under **<Exchange 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.

## 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 as to the Administrators group on the SiteScope server.

- a. Click **Start > Administrative Tools > Server Manager**.
- b. Expand the **Configuration > Local Users and Groups** folder in the left pane, and click the **Groups** folder.
- c. Double-click the **Administrators** group icon to open the Administrators Properties window.
- d. Click the **Add** button to add each Mailbox Owner you expect to use with the Exchange monitor.

## 3. Verify that the SiteScope user logon is a member of Administrators group or a domain administrator account and delegated the Exchange Server Administrators role

**Caution:** The SiteScope user account must be a Local Administrator or a member of the domain admins group and delegated the Exchange Server Administrators role.

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.

## How to Configure the Microsoft Exchange Base Monitor

### 1. Prerequisites

- Make sure you prepared the system for using the Microsoft Exchange monitor as described in ["How to Prepare the System for Using the Microsoft Exchange Base Monitor" on the previous page.](#)

- Exchange Management Shell must be installed on the SiteScope server. Windows PowerShell 2.0 must be installed on the computer that runs the Exchange Management Shell.
- To run each cmdlet, the server roles that correspond to the cmdlets you want to run must be installed on the Microsoft Exchange Server. When monitoring Microsoft Exchange Server 2010 or 2013, 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.

For Microsoft Exchange Server 2013:

Server Role	Cmdlet
Mailbox	<ul style="list-style-type: none"> <li>◦ <b>Get-StoreUsageStatistics</b></li> <li>◦ <b>Test-AssistantHealth</b></li> <li>◦ <b>Test-ExchangeSearch</b></li> <li>◦ <b>Test-MailFlow</b></li> <li>◦ <b>Test-MapiConnectivity</b></li> <li>◦ <b>Test-ReplicationHealth</b></li> </ul>
Mailbox, Client Access	<b>Test-ServiceHealth</b>
Client Access	<ul style="list-style-type: none"> <li>◦ <b>Test-MRSHealth</b></li> <li>◦ <b>Test-CalendarConnectivity</b></li> <li>◦ <b>Test-WebServicesConnectivity</b></li> <li>◦ <b>Test-ImapConnectivity</b></li> <li>◦ <b>Test-PopConnectivity</b></li> <li>◦ <b>Test-PowerShellConnectivity</b></li> <li>◦ <b>Test-ActiveSyncConnectivity</b></li> <li>◦ <b>Test-OutlookWebServices</b></li> </ul>

For Microsoft Exchange Server 2010:

Server Role	Cmdlet
Mailbox	<ul style="list-style-type: none"> <li>◦ <b>Test-MAPIConnectivity</b></li> <li>◦ <b>Test-ExchangeSearch</b></li> </ul>
Hub Transport, Mailbox	<b>Test-MailFlow</b>
Client Access	<ul style="list-style-type: none"> <li>◦ <b>Test-OWAConnectivity</b></li> <li>◦ <b>Test-WebServicesConnectivity</b></li> </ul>

## 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## 3. 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 15 minutes.

## UI Descriptions

### Microsoft Exchange Base Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Exchange server</b>	Name of the server running Microsoft Exchange Server that you want to monitor.
<b>Exchange domain</b>	Domain name and the mailbox of the server running Microsoft Exchange Server that you want to monitor.
<b>Mailbox</b>	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>Remote Exchange script file path</b>	Full path to the Microsoft Exchange Server Management Shell script file. <b>Example:</b> C:\Program Files\Microsoft\Exchange Server\V15\Bin\RemoteExchange.ps1
<b>Timeout (seconds)</b>	Amount of time to wait, in seconds, for getting a response. You can set the timeout to no less than 1 second and no more than 15 minutes. <b>Default value:</b> 600 seconds
<b>PowerShell virtual directory name</b>	Name of the PowerShell virtual directory that is used by <b>Test-PowerShellConnectivity</b> cmdlet. <b>Default value:</b> Power Shell (Default Web Site)
<b>POP3 service port</b>	POP3 service port is used by the <b>Test-POPConnectivity</b> cmdlet. <b>Default value:</b> 995 SSL or 110 for plain text /TLS.
<b>IMAP4 service port</b>	IMAP4 service port is used by the <b>Test-ImapConnectivity</b> cmdlet. <b>Default value:</b> 993 for SSL or 143 for plain text /TLS.

UI Element	Description
<b>Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Counters are displayed in the counters tree if the role (required for the corresponding cmdlet) is installed on the monitored server. For role details, see “Prerequisites” in <a href="#">"How to Configure the Microsoft Exchange Base Monitor" on page 401</a>.</p> <p>Counter values are calculated from the output of the corresponding cmdlet. Cmdlet output processing can be as follows:</p> <ul style="list-style-type: none"><li>• Normalization of found value (for example, move to another units)</li><li>• Summation of the found values with same name.</li><li>• Average value from found values with the same name.</li></ul>
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

**For Microsoft Exchange Server 2013 only:**

**Test-AssistantHealth**

Assistant Performance Counters\EventsInDatabaseQueues  
Assistant Performance Counters\CrashDumpCount

**Get-StoreUsageStatistics**

Store Usage Statistics\TimeInCPU  
Store Usage Statistics\TimeInServer

**Test-CalendarConnectivity**

Calendar Connectivity\Logon\Result  
Calendar Connectivity\Logon\Latency  
Calendar Connectivity\CalendarHTML\Result  
Calendar Connectivity\CalendarHTML\Latency  
Calendar Connectivity\CalendarICS\Result  
Calendar Connectivity\CalendarICS\Latency

**Test-ImapConnectivity**

IMAP4 Connectivity\Result  
IMAP4 Connectivity\Latency

**Test-PopConnectivity**

POP3 Connectivity\Result  
POP3 Connectivity\Latency

**Test-PowerShellConnectivity**

PowerShell Connectivity\Result  
PowerShell Connectivity\Latency

**Test-MRSHealth**

Test MRS Health\ServiceCheckPassed  
Test MRS Health\RPCPingCheckPassed  
Test MRS Health\QueueScanCheckPassed

**Test-ReplicationHealth**

Replication Health\ClusterServiceCheckResult  
Replication Health\ReplayServiceCheckResult  
Replication Health\ActiveManagerCheckResult  
Replication Health\TasksRpcListenerCheckResult  
Replication Health\TcpListenerCheckResult  
Replication Health\ServerLocatorServiceCheckResult  
Replication Health\DagMembersUpCheckResult  
Replication Health\ClusterNetworkCheckResult  
Replication Health\QuorumGroupCheckResult  
Replication Health\DatabaseRedundancyCheckResult  
Replication Health\DatabaseAvailabilityCheckResult  
Replication Health\DBCopysuspendedCheckResult  
Replication Health\DBCopysFailedCheckResult  
Replication Health\DBInitializingCheckResult  
Replication Health\DBDisconnectedCheckResult  
Replication Health\DBLogCopyKeepingUpCheckResult  
Replication Health\DBLogReplayKeepingUpCheckResult

**Test-ServiceHealth**

Service Health\ServicesNotRunning

**Test-WebServicesConnectivity**

Web Services Connectivity\EwsGetFolder\Result  
Web Services Connectivity\EwsGetFolder\Latency  
Web Services Connectivity\AutoDiscoverSoapProvider\Result

Web Services Connectivity\AutoDiscoverSoapProvider\Latency

**Test-ActiveSyncConnectivity**

Active Sync Connectivity\Options\Result  
Active Sync Connectivity\Options\Latency  
Active Sync Connectivity\FolderSync\Result  
Active Sync Connectivity\FolderSync\Latency  
Active Sync Connectivity\First Sync\Result  
Active Sync Connectivity\First Sync\Latency  
Active Sync Connectivity\GetItemEstimate\Result  
Active Sync Connectivity\GetItemEstimate\Latency  
Active Sync Connectivity\Sync Data\Result  
Active Sync Connectivity\Sync Data\Latency  
Active Sync Connectivity\Ping\Result  
Active Sync Connectivity\Ping\Latency  
Active Sync Connectivity\Sync Test Item\Result  
Active Sync Connectivity\Sync Test Item\Latency

**Test-OutlookWebServices**

Outlook Web Services\AutoDiscoverOutlookProvider\Result  
Outlook Web Services\AutoDiscoverOutlookProvider\Latency  
Outlook Web Services\ExchangeWebServices\Result  
Outlook Web Services\ExchangeWebServices\Latency  
Outlook Web Services\AvailabilityService\Result  
Outlook Web Services\AvailabilityService\Latency  
Outlook Web Services\OfflineAddressBook\Result  
Outlook Web Services\OfflineAddressBook\Latency

**For Microsoft Exchange Server 2010 and 2013:**

**Test-ExchangeSearch**

Exchange Search\ResultFound  
Exchange Search\SearchTimeInSeconds

**Test-Mailflow**

Mail Flow\TestMailflowResult  
Mail Flow\MessageLatencyTime

**Test-MAPIConnectivity**

MAPI Connectivity\Result  
MAPI Connectivity\Latency

**For Microsoft Exchange Server 2010 only:**

**Test-WebServicesConnectivity**

Web Services Connectivity\GetFolder\Result  
Web Services Connectivity\GetFolder\Latency  
Web Services Connectivity\SyncFolderItems\Result  
Web Services Connectivity\SyncFolderItems\Latency  
Web Services Connectivity\CreateItem\Result  
Web Services Connectivity\CreateItem\Latency  
Web Services Connectivity\DeleteItem\Result  
Web Services Connectivity\DeleteItem\Latency  
Test-OWAConnectivity  
OWA Connectivity\Result  
OWA Connectivity\Latency

**Test-OWAConnectivity**

OWA Connectivity\Result  
OWA Connectivity\Latency

## Tips/Troubleshooting

### Unable to Connect to Microsoft Exchange Server 2010 and Receive Counters

If you are unable to connect to the Microsoft Exchange Server 2013 and receive counters, make sure you have the correct PowerShell startup parameters.

1. Open PowerShell and type the following to create a default PowerShell profile applicable to all users and automatically load the Exchange snap-in:  

```
if (!(test-path $profile.AllUsersAllHosts)) {new-item -type file -path  
$profile.AllUsersAllHosts -force}  
notepad $profile.AllUsersAllHosts
```
2. Add the following syntax to the **\$profile.AllUsersAllHosts** file:  

```
. $env:ExchangeInstallPath\bin\RemoteExchange.ps1  
Connect-ExchangeServer -auto
```
3. Save your changes and exit PowerShell.
4. Restart the SiteScope service.
5. Go into SiteScope and define the Microsoft Exchange monitor as described in the UI Descriptions section above.

### Microsoft Exchange Base Monitor might not work on 64-bit version of Windows Server 2008

In some cases, the Microsoft Exchange Base Monitor might not work on a 64-bit version of Windows Server 2008. This can occur when a 32-bit application is unable to access the system32 folder on a computer running a 64-bit version of Windows Server 2008.

**Workaround:** In **Preferences > Infrastructure Preferences > General Settings**, make sure you entered the correct PowerShell execute command in the **Power Shell execute command** box. For example:

C:\Windows\Sysnative\WindowsPowerShell\v1.0\powershell.exe

# Chapter 55: Microsoft Exchange 2000/2003/2007 Message Traffic Monitor

**Note:** The Microsoft Exchange 2000 and 2003 Message Traffic monitors were deprecated, and the Microsoft Exchange 2000 and 2003 solution templates are no longer available. If these monitors were configured in a previous version of SiteScope, they will still work after performing a SiteScope upgrade (but we do not recommend using them). We recommend migrating to the Microsoft Exchange 2007 monitor.

Use the Microsoft Exchange Message Traffic monitor to display important statistics about messages handled by a Microsoft Exchange 2007 server, such as a count of messages sent that are larger than a certain size, or sent to a large number of recipients.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of Microsoft Exchange Server monitoring. For details, see Microsoft Exchange Solution Templates in the Using SiteScope Guide.

## To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click the Microsoft Exchange solution template version that you require, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

## Learn About

### Supported Platforms/Versions

This monitor is supported in SiteScopes that are running on Windows versions only.

### License Consumption

Points-based Usage	Capacity-based Usage
Five points per monitor	One OSi license per monitored host Note: This monitor is not available when using Community edition.

## Tasks

### How to Configure the Microsoft Exchange Message Traffic Monitor

1. Prerequisites
  - This monitor requires the Microsoft Exchange solution templates to enable it in the SiteScope interface.



- 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.
2. Deploy the Microsoft Exchange Solution template  
This monitor can only be added by deploying the Microsoft Exchange solution template version that you require. For information about using templates to deploy monitors, see SiteScope Templates in the Using SiteScope Guide.
  3. Configure the monitor properties  
After the monitor has been created, you can edit the monitor configuration in the same way as other monitors. Since this monitor returns statistics that do not normally change very rapidly and are not critical to system availability, it should be scheduled to run infrequently, or on demand only.  
Configure the monitor properties as required.  
For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Microsoft Exchange Message Traffic Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Recipient limit</b>	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>	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>	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>	Number (N) of domains to use for reporting the top N sending domains. <b>Default value:</b> 5
<b>Number of outgoing users</b>	Number (N) of users to use for reporting the top N outgoing users. <b>Default value:</b> 5

UI Element	Description
<b>Log directory</b>	UNC path of the messaging tracking log file directory. <b>Default value:</b> \\<server name>\MessageTracking <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>
<b>Reporting directory</b>	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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Chapter 56: Microsoft Exchange 5.5 Message Traffic Monitor (Deprecated)

**Note:** The Microsoft Exchange 5.5 Message Traffic monitor was deprecated, and the Microsoft Exchange 5.5 solution template is no longer available. If this monitor was configured in a previous version of SiteScope, it will still work after performing a SiteScope upgrade (but we do not recommend using it). We recommend migrating to the Microsoft Exchange 2007 Message Traffic monitor or later.

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. 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.

**Note:**

- This monitor is not available when using Community edition.
- To use the monitor, you must have an Operating System Instance (OSi) license with sufficient available capacity. For license purchase inquiries (or if you require additional capacity), contact your HPE sales representative or use the “Contact Us” link in the [HPE SiteScope Product page](#).

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of Microsoft Exchange Server monitoring. For details, see Microsoft Exchange Solution Templates in the Using SiteScope Guide.

## To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click **Microsoft Exchange 5.5**, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

## Tasks

### How to Configure the Microsoft Exchange 5.5 Message Traffic Monitor

#### 1. Prerequisites

- This monitor requires the Microsoft Exchange solution templates to enable it in the SiteScope interface.
- The Microsoft Exchange 5.5 Message Traffic monitor requires additional licensing to enable the monitor type in the SiteScope interface. For license purchase inquiries (or if you require additional capacity), contact your HPE sales representative or use the “Contact Us” link in the [HPE SiteScope Product page](#).

#### 2. Deploy the Microsoft Exchange Solution template

This monitor can only be added by deploying the Microsoft Exchange 5.5 solution template. For information about using templates to deploy monitors, see SiteScope Templates in the Using SiteScope Guide.

3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors.

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Microsoft Exchange 5.5 Message Traffic Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Recipient limit</b>	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>	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>	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>	Number (N) of domains to use for reporting the top N sending domains. <b>Default value:</b> 5
<b>Number of outgoing users</b>	Number (N) of users to use for reporting the top N outgoing users. <b>Default value:</b> 5
<b>Log directory</b>	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>	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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Chapter 57: Microsoft Exchange 2003 Mailbox Monitor (Deprecated)

**Note:** The Microsoft Exchange 2003 Mailbox monitor was deprecated, and the Microsoft Exchange 2003 solution template is no longer available. If this monitor was configured in a previous version of SiteScope, it is still displayed in SiteScope after performing an upgrade (but will not work). We recommend migrating to a Microsoft Exchange 2007 or later monitor.

The Microsoft Exchange 2003 Mailbox monitor enables you to monitor mailbox statistics of Microsoft Exchange Server 2003. 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.

**Note:** This monitor is not available when using Community edition.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of Microsoft Exchange Server monitoring. For details, see Microsoft Exchange Solution Templates in the Using SiteScope Guide.

## To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click **Microsoft Exchange 2003**, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

## Learn About

### Supported Platforms/Versions

This monitor is supported in SiteScopes that are running on Windows versions only.

## Tasks

### How to Configure the Microsoft Exchange 2003 Mailbox Monitor

1. Prerequisites
  - This monitor requires the Microsoft Exchange solution templates to enable it in the SiteScope interface.
  - 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.
2. Deploy the Microsoft Exchange Solution template

This monitor can only be added by deploying the Microsoft Exchange 2003 solution template. For information about using templates to deploy monitors, see SiteScope Templates in the Using SiteScope Guide.

3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors.

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Microsoft Exchange 2003 Mailbox Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	Server running Microsoft Exchange Server 2003 that you want to monitor.
<b>User name</b>	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>	Password for the user name entered above, or blank if user name is blank.
<b>N largest mailboxes</b>	Number (N) of mailboxes to display when reporting the N largest mailboxes.  <b>Default value:</b> 5
<b>Days since access</b>	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>	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>	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

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### 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>).

# Chapter 58: Microsoft Exchange 2003 Public Folder Monitor (Deprecated)

**Note:** The Microsoft Exchange 2003 Public Folder monitor was deprecated, and the Microsoft Exchange 2003 solution template is no longer available. If this monitor was configured in a previous version of SiteScope, it is still displayed in SiteScope after performing an upgrade (but will not work). We recommend migrating to a Microsoft Exchange 2007 or later monitor.

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:** This monitor is not available when using Community edition.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of Microsoft Exchange Server monitoring. For details, see Microsoft Exchange Solution Templates in the Using SiteScope Guide.

## To access

Select the **Templates** context. In the template tree, expand the **Solution Templates** container. Right-click **Microsoft Exchange 2003**, and select **Deploy Template**. Select the SiteScope group container into which you want to deploy the solution template, and enter the deployment values.

## Learn About

### Supported Platforms/Versions

This monitor is supported in SiteScopes that are running on Windows versions only.

## Tasks

### How to Configure the Microsoft Exchange 2003 Public Folder Monitor

1. Prerequisites
  - This monitor requires the Microsoft Exchange solution templates to enable it in the SiteScope interface.
  - 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.
2. Deploy the Microsoft Exchange Solution template



This monitor can only be added by deploying the Microsoft Exchange 2003 solution template version that you require. For information about using templates to deploy monitors, see SiteScope Templates in the Using SiteScope Guide.

3. Configure the monitor properties

After the monitor has been created, you can edit the monitor configuration in the same way as other monitors. Since this monitor returns statistics that do not normally change very rapidly and are not critical to system availability, it should be scheduled to run infrequently, or on demand only.

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Microsoft Exchange 2003 Public Folder Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	Name of the server running Microsoft Exchange Server 2003 that you want to monitor.
<b>User name</b>	User name to use when querying the server for mailbox 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.  <b>Default value:</b> If this box is left blank, the user that SiteScope is running as is used.
<b>Password</b>	Password for the user name entered above, or blank if user name is blank.
<b>Days since access</b>	Number of days (N) to use when reporting the number of public folders that have not been accessed in N days.  <b>Default value:</b> 7
<b>Timeout (seconds)</b>	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
<b>Reporting directory</b>	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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Chapter 59: Microsoft Hyper-V Monitor

This monitor enables you to monitor performance statistics of the Microsoft Hyper-V infrastructure for various server applications.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Hyper-V monitor.

## Learn About

This section includes:

- ["Microsoft Hyper-V Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" on the next page](#)

### Microsoft Hyper-V Monitor Overview

Use the Microsoft Hyper-V monitor to monitor vital performance metrics in Hyper-V environments. Microsoft Hyper-V is a server virtualization that runs on Windows 2008 or higher. It is a hypervisor-based virtualization system for x64 Windows operating systems. The Microsoft Hyper-V monitor enables monitoring of Microsoft Hyper-V hosts and virtual machines.

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 Microsoft Hyper-V monitor instance for each Hyper-V Server in your environment. The error and warning thresholds for the monitor can be set on one or more Microsoft Hyper-V Server performance statistics. The Microsoft Hyper-V monitor makes use of performance objects and counters to measure application server performance.

### Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1. All these supported operating systems should be with Hyper-V role enabled.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

### IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

## Tasks

### How to Configure the Microsoft Hyper-V Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Microsoft Hyper-V Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of 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></p> <ul style="list-style-type: none"><li>• 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 in the Using SiteScope Guide.</li><li>• When working in template mode, 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></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

UI Element	Description
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 <a href="#">How to Configure SiteScope to Monitor a Remote Microsoft Windows Server</a> in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see <a href="#">New/Edit Microsoft Windows Remote Server Dialog Box</a> in the Using SiteScope Guide.</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>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see [Common Monitor Settings](#) in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<p><b>Hyper-V Hypervisor</b></p> <ul style="list-style-type: none"> <li>• Logical Processors</li> <li>• Monitored Notifications</li> <li>• Partitions</li> <li>• Total Pages</li> <li>• Virtual Processors</li> </ul> <p><b>Hyper-V Hypervisor Logical Processor</b></p> <ul style="list-style-type: none"> <li>• % C1 Time</li> <li>• % C2 Time</li> <li>• % C3 Time</li> <li>• % Guest Run Time</li> <li>• % Hypervisor Run Time</li> <li>• % Idle Time</li> <li>• % Total Run Time</li> <li>• C1 Transitions/sec</li> <li>• C2 Transitions/sec</li> <li>• C3 Transitions/sec</li> <li>• Context Switches/sec</li> <li>• Hardware Interrupts/sec</li> <li>• Inter-Processor Interrupts Sent/sec</li> <li>• Inter-Processor Interrupts/sec</li> <li>• Monitor Transition Cost</li> <li>• Scheduler Interrupts/sec</li> <li>• Timer Interrupts/sec</li> <li>• Total Interrupts/sec</li> </ul> <p><b>Hyper-V Hypervisor Root Partition</b></p> <ul style="list-style-type: none"> <li>• 1G GPA pages</li> <li>• 2M GPA pages</li> <li>• 4K GPA pages</li> <li>• Address Spaces</li> <li>• Deposited Pages</li> <li>• GPA Pages</li> <li>• GPA Space Modifications/sec</li> <li>• Recommended Virtual TLB Size</li> <li>• Virtual Processors</li> <li>• Virtual TLB Flush Entireties/sec</li> <li>• Virtual TLB Pages</li> </ul>	<p><b>Hyper-V Hypervisor Root Virtual Processor</b></p> <ul style="list-style-type: none"> <li>• % Guest Run Time</li> <li>• % Hypervisor Run Time</li> <li>• % Total Run Time</li> <li>• APIC EOI Accesses/sec</li> <li>• APIC IPIs Sent/sec</li> <li>• APIC MMIO Accesses/sec</li> <li>• APIC Self IPIs Sent/sec</li> <li>• APIC TPR Accesses/sec</li> <li>• Address Domain Flushes/sec</li> <li>• Address Space Evictions/sec</li> <li>• Address Space Flushes/sec</li> <li>• Address Space Switches/sec</li> <li>• CPUID Instructions Cost</li> <li>• CPUID Instructions/sec</li> <li>• Control Register Accesses Cost</li> <li>• Control Register Accesses/sec</li> <li>• Debug Register Accesses Cost</li> <li>• Debug Register Accesses/sec</li> <li>• Emulated Instructions Cost</li> <li>• Emulated Instructions/sec</li> <li>• External Interrupts Cost</li> <li>• External Interrupts/sec</li> <li>• GPA Space Hypercalls/sec</li> <li>• Global GVA Range Flushes/sec</li> <li>• Guest Page Table Maps/sec</li> <li>• HLT Instructions Cost</li> <li>• HLT Instructions/sec</li> <li>• Hypercalls Cost</li> <li>• Hypercalls/sec</li> <li>• IO Instructions Cost</li> <li>• IO Instructions/sec</li> <li>• IO Intercept Messages/sec</li> <li>• Large Page TLB Fills/sec</li> <li>• Local Flushed GVA Ranges/sec</li> <li>• Logical Processor Hypercalls/sec</li> <li>• Logical Processor Migrations/sec</li> <li>• Long Spin Wait Hypercalls/sec</li> <li>• MSR Accesses Cost</li> <li>• MSR Accesses/sec</li> <li>• MWAIT Instructions Cost</li> </ul>	<ul style="list-style-type: none"> <li>• MWAIT Instructions/sec</li> <li>• Memory Intercept Messages/sec</li> <li>• Other Hypercalls/sec</li> <li>• Other Intercepts Cost</li> <li>• Other Intercepts/sec</li> <li>• Other Messages/sec</li> <li>• Page Fault Intercepts Cost</li> <li>• Page Fault Intercepts/sec</li> <li>• Page Invalidations Cost</li> <li>• Page Invalidations/sec</li> <li>• Page Table Allocations/sec</li> <li>• Page Table Evictions/sec</li> <li>• Page Table Reclamations/sec</li> <li>• Page Table Resets/sec</li> <li>• Page Table Validations/sec</li> <li>• Page Table Write Intercepts/sec</li> <li>• Pending Interrupts Cost</li> <li>• Pending Interrupts/sec</li> <li>• Reflected Guest Page Faults/sec</li> <li>• Small Page TLB Fills/sec</li> <li>• Synthetic Interrupt Hypercalls/sec</li> <li>• Synthetic Interrupts/sec</li> <li>• Total Intercepts Cost</li> <li>• Total Intercepts/sec</li> <li>• Total Messages/sec</li> <li>• Virtual Interrupt Hypercalls/sec</li> <li>• Virtual Interrupts/sec</li> <li>• Virtual MMU Hypercalls/sec</li> <li>• Virtual Processor Hypercalls/sec</li> </ul> <p><b>Hyper-V Hypervisor Virtual Processor</b></p> <ul style="list-style-type: none"> <li>• % Guest Run Time</li> <li>• % Hypervisor Run Time</li> <li>• % Total Run Time</li> <li>• APIC EOI Accesses/sec</li> <li>• APIC IPIs Sent/sec</li> <li>• APIC MMIO Accesses/sec</li> <li>• APIC Self IPIs Sent/sec</li> <li>• APIC TPR Accesses/sec</li> <li>• Address Domain Flushes/sec</li> <li>• Address Space Evictions/sec</li> <li>• Address Space Flushes/sec</li> <li>• Address Space Switches/sec</li> <li>• CPUID Instructions Cost</li> <li>• CPUID Instructions/sec</li> </ul>
--	---	---

<ul style="list-style-type: none"> <li>• Control Register Accesses Cost</li> <li>• Control Register Accesses/sec</li> <li>• Debug Register Accesses Cost</li> <li>• Debug Register Accesses/sec</li> <li>• Emulated Instructions Cost</li> <li>• Emulated Instructions/sec</li> <li>• External Interrupts Cost</li> <li>• External Interrupts/sec</li> <li>• GPA Space Hypercalls/sec</li> <li>• Global GVA Range Flushes/sec</li> <li>• Guest Page Table Maps/sec</li> <li>• HLT Instructions Cost</li> <li>• HLT Instructions/sec</li> <li>• Hypercalls Cost</li> <li>• Hypercalls/sec</li> <li>• IO Instructions Cost</li> <li>• IO Instructions/sec</li> <li>• IO Intercept Messages/sec</li> <li>• Large Page TLB Fills/sec</li> <li>• Local Flushed GVA Ranges/sec</li> <li>• Logical Processor Hypercalls/sec</li> <li>• Logical Processor Migrations/sec</li> <li>• Long Spin Wait Hypercalls/sec</li> <li>• MSR Accesses Cost</li> <li>• MSR Accesses/sec</li> <li>• MWAIT Instructions Cost</li> <li>• MWAIT Instructions/sec</li> <li>• Memory Intercept Messages/sec</li> <li>• Other Hypercalls/sec</li> <li>• Other Intercepts Cost</li> <li>• Other Intercepts/sec</li> <li>• Other Messages/sec</li> <li>• Page Fault Intercepts Cost</li> <li>• Page Fault Intercepts/sec</li> <li>• Page Invalidations Cost</li> <li>• Page Invalidations/sec</li> <li>• Page Table Allocations/sec</li> <li>• Page Table Evictions/sec</li> <li>• Page Table Reclamations/sec</li> <li>• Page Table Resets/sec</li> <li>• Page Table Validations/sec</li> <li>• Page Table Write Intercepts/sec</li> <li>• Pending Interrupts Cost</li> <li>• Pending Interrupts/sec</li> </ul>	<ul style="list-style-type: none"> <li>• Reflected Guest Page Faults/sec</li> <li>• Small Page TLB Fills/sec</li> <li>• Synthetic Interrupt Hypercalls/sec</li> <li>• Synthetic Interrupts/sec</li> <li>• Total Intercepts Cost</li> <li>• Total Intercepts/sec</li> <li>• Total Messages/sec</li> <li>• Virtual Interrupt Hypercalls/sec</li> <li>• Virtual Interrupts/sec</li> <li>• Virtual MMU Hypercalls/sec</li> <li>• Virtual Processor Hypercalls/sec</li> </ul> <p><b>Hyper-V Task Manager Detail</b></p> <ul style="list-style-type: none"> <li>• Add Resources Virtual Machine Tasks Completed</li> <li>• Add Resources Virtual Machine Tasks Recent Time</li> <li>• Add Resources Virtual Machine Tasks in Progress</li> <li>• Apply Snapshot Virtual Machine Tasks Completed</li> <li>• Apply Snapshot Virtual Machine Tasks Recent Time</li> <li>• Apply Snapshot Virtual Machine Tasks in Progress</li> <li>• Clone Virtual Machine Tasks Completed</li> <li>• Clone Virtual Machine Tasks Recent Time</li> <li>• Clone Virtual Machine Tasks in Progress</li> <li>• Create VSS Snapshot Set Tasks Completed</li> <li>• Create VSS Snapshot Set Tasks Recent Time</li> <li>• Create VSS Snapshot Set Tasks in Progress</li> <li>• Define Virtual Machine Tasks Completed</li> <li>• Define Virtual Machine Tasks Recent Time</li> <li>• Define Virtual Machine Tasks in Progress</li> <li>• Destroy Snapshot Virtual Machine Tasks Completed</li> <li>• Destroy Snapshot Virtual Machine Tasks Recent Time</li> <li>• Destroy Snapshot Virtual Machine Tasks in Progress</li> <li>• Destroy Virtual Machine Tasks Completed</li> <li>• Destroy Virtual Machine Tasks Recent Time</li> <li>• Destroy Virtual Machine Tasks in Progress</li> </ul>	<ul style="list-style-type: none"> <li>• Export Virtual Machine Tasks Completed</li> <li>• Export Virtual Machine Tasks Recent Time</li> </ul> <ul style="list-style-type: none"> <li>• Export Virtual Machine Tasks in Progress</li> <li>• Import Virtual Machine Tasks Completed</li> <li>• Import Virtual Machine Tasks Recent Time</li> </ul> <ul style="list-style-type: none"> <li>• Import Virtual Machine Tasks in Progress</li> <li>• Merge Disk Tasks Completed</li> <li>• Merge Disk Tasks Recent Time</li> <li>• Merge Disk Tasks in Progress</li> <li>• Migrate Virtual Machine Tasks Completed</li> <li>• Migrate Virtual Machine Tasks Recent Time</li> <li>• Migrate Virtual Machine Tasks in Progress</li> <li>• Modify Resources Virtual Machine Tasks Completed</li> <li>• Modify Resources Virtual Machine Tasks Recent Time</li> <li>• Modify Resources Virtual Machine Tasks in Progress</li> <li>• Modify Service Settings Tasks Completed</li> <li>• Modify Service Settings Tasks Recent Time</li> <li>• Modify Service Settings Tasks in Progress</li> <li>• Modify Virtual Machine Tasks Completed</li> <li>• Modify Virtual Machine Tasks Recent Time</li> </ul> <ul style="list-style-type: none"> <li>• Modify Virtual Machine Tasks in Progress</li> <li>• Pause Virtual Machine Tasks Completed</li> <li>• Pause Virtual Machine Tasks Recent Time</li> <li>• Pause Virtual Machine Tasks in Progress</li> <li>• Remove Resources Virtual Machine Tasks Completed</li> <li>• Remove Resources Virtual Machine Tasks Recent Time</li> <li>• Remove Resources Virtual Machine Tasks in Progress</li> <li>• Reset Virtual Machine Tasks Completed</li> <li>• Reset Virtual Machine Tasks Recent Time</li> <li>• Reset Virtual Machine Tasks in Progress</li> </ul>
--	---	--

<ul style="list-style-type: none"> <li>• Restore Virtual Machine Tasks Completed</li> <li>• Restore Virtual Machine Tasks Recent Time</li> <li>• Restore Virtual Machine Tasks in Progress</li> <li>• Resume Virtual Machine Tasks Completed</li> <li>• Resume Virtual Machine Tasks Recent Time</li> <li>• Resume Virtual Machine Tasks in Progress</li> <li>• Save Virtual Machine Tasks Completed</li> </ul> <ul style="list-style-type: none"> <li>• Save Virtual Machine Tasks Recent Time</li> <li>• Save Virtual Machine Tasks in Progress</li> </ul> <ul style="list-style-type: none"> <li>• Shutdown Virtual Machine Tasks Completed</li> <li>• Shutdown Virtual Machine Tasks Recent Time</li> <li>• Shutdown Virtual Machine Tasks in Progress</li> <li>• Snapshot Virtual Machine Tasks Completed</li> <li>• Snapshot Virtual Machine Tasks Recent Time</li> <li>• Snapshot Virtual Machine Tasks in Progress</li> <li>• Start Virtual Machine Tasks Completed</li> <li>• Start Virtual Machine Tasks Recent Time</li> <li>• Start Virtual Machine Tasks in Progress</li> </ul> <ul style="list-style-type: none"> <li>• Waiting to Start Virtual Machine Tasks Completed</li> <li>• Waiting to Start Virtual Machine Tasks Recent Time</li> <li>• Waiting to Start Virtual Machine Tasks in Progress</li> </ul> <b>Hyper-V VM Vid Numa Node</b> <ul style="list-style-type: none"> <li>• PageCount</li> <li>• ProcessorCount</li> </ul> Hyper-V VM Vid Partition <ul style="list-style-type: none"> <li>• Physical Pages Allocated</li> <li>• Preferred NUMA Node Index</li> <li>• Remote Physical Pages</li> </ul> <b>Hyper-V Virtual IDE Controller</b> <ul style="list-style-type: none"> <li>• Read Bytes/sec</li> <li>• Read Sectors/sec</li> <li>• Write Bytes/sec</li> <li>• Written Sectors/sec</li> </ul>	<b>Hyper-V Virtual Machine Bus</b> <ul style="list-style-type: none"> <li>• Interrupts Received</li> <li>• Interrupts Sent</li> <li>• Throttle Events</li> </ul> <b>Hyper-V Virtual Machine Health Summary</b> <ul style="list-style-type: none"> <li>• Health Critical</li> <li>• Health Ok</li> </ul> <b>Hyper-V Virtual Machine Summary</b> <ul style="list-style-type: none"> <li>• Applying Snapshot</li> <li>• Deleting</li> <li>• Deleting Saved State</li> <li>• Deleting Snapshot</li> <li>• Exporting</li> <li>• Merging Disks</li> <li>• Paused</li> <li>• Pausing</li> <li>• Resetting</li> <li>• Resuming</li> <li>• Running</li> <li>• Saved</li> <li>• Saving</li> <li>• Starting</li> <li>• Stopping</li> <li>• Taking Snapshot</li> <li>• Turned Off</li> <li>• Waiting to Start</li> </ul> <b>Hyper-V Virtual Network Adapter</b> <ul style="list-style-type: none"> <li>• Broadcast Packets Received/sec</li> <li>• Broadcast Packets Sent/sec</li> <li>• Bytes Received/sec</li> <li>• Bytes Sent/sec</li> <li>• Bytes/sec</li> <li>• Directed Packets Received/sec</li> <li>• Directed Packets Sent/sec</li> <li>• Multicast Packets Received/sec</li> <li>• Multicast Packets Sent/sec</li> <li>• Packets Received/sec</li> <li>• Packets Sent/sec</li> <li>• Packets/sec</li> </ul> <b>Hyper-V Virtual Storage Device</b> <ul style="list-style-type: none"> <li>• Error Count</li> <li>• Flush Count</li> <li>• Read Bytes/sec</li> <li>• Read Count</li> <li>• Write Bytes/sec</li> <li>• Write Count</li> </ul>	<b>Hyper-V Virtual Switch</b> <ul style="list-style-type: none"> <li>• Broadcast Packets Received/sec</li> <li>• Broadcast Packets Sent/sec</li> <li>• Bytes Received/sec</li> <li>• Bytes Sent/sec</li> <li>• Bytes/sec</li> <li>• Directed Packets Received/sec</li> <li>• Directed Packets Sent/sec</li> <li>• Learned Mac Addresses</li> <li>• Learned Mac Addresses/sec</li> <li>• Multicast Packets Received/sec</li> <li>• Multicast Packets Sent/sec</li> <li>• Packets Flooded</li> <li>• Packets Flooded/sec</li> <li>• Packets Received/sec</li> <li>• Packets Sent/sec</li> <li>• Packets/sec</li> <li>• Purged Mac Addresses</li> <li>• Purged Mac Addresses/sec</li> </ul> Hyper-V Virtual Switch Port <ul style="list-style-type: none"> <li>• Broadcast Packets Received/sec</li> <li>• Broadcast Packets Sent/sec</li> <li>• Bytes Received/sec</li> <li>• Bytes Sent/sec</li> <li>• Bytes/sec</li> <li>• Directed Packets Received/sec</li> <li>• Directed Packets Sent/sec</li> <li>• Multicast Packets Received/sec</li> <li>• Multicast Packets Sent/sec</li> <li>• Packets Received/sec</li> <li>• Packets Sent/sec</li> <li>• Packets/sec</li> <li>• Broadcast Packets Received/sec</li> <li>• Broadcast Packets Sent/sec</li> <li>• Bytes Received/sec</li> <li>• Bytes Sent/sec</li> <li>• Bytes/sec</li> <li>• Directed Packets Received/sec</li> <li>• Directed Packets Sent/sec</li> <li>• Multicast Packets Received/sec</li> <li>• Multicast Packets Sent/sec</li> <li>• Packets Received/sec</li> <li>• Packets Sent/sec</li> <li>• Packets/sec</li> <li>• Broadcast Packets Received/sec</li> <li>• Broadcast Packets Sent/sec</li> <li>• Bytes Received/sec</li> <li>• Bytes Sent/sec</li> <li>• Bytes/sec</li> <li>• Directed Packets Received/sec</li> <li>• Directed Packets Sent/sec</li> <li>• Multicast Packets Received/sec</li> <li>• Multicast Packets Sent/sec</li> <li>• Packets Received/sec</li> <li>• Packets Sent/sec</li> <li>• Packets/sec</li> </ul>
---	---	--

## Tips/Troubleshooting

### General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.



# Chapter 60: Microsoft IIS Server Monitor

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 error and warning thresholds for the monitor can be set on one or more IIS server performance counters.

**Tip:** 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 Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft IIS Server monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)
- ["Microsoft IIS Server Topology" on the next page](#)
- ["License Consumption" on page 427](#)

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- The Microsoft IIS Server monitor supports monitoring the following:
  - HTTP/HTTPS services on IIS 4.0, 5.0, 7.0, 7.5, 8.0, 8.5.
  - HTTP/HTTPS, FTP, NNTP and MSMQ Queue on IIS 6, 7.0, 8.0, 8.5.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

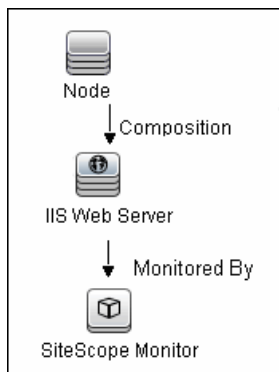
For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## Microsoft IIS Server Topology

The Microsoft IIS Server monitor can identify the topology of the Microsoft IIS Server being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

# Tasks

## How to Configure the Microsoft IIS Server Monitor

### 1. Prerequisites

- Make sure you have the specific access permissions required for this monitor as specified in Permissions and Credentials.
- 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.

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

### 3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["Microsoft IIS Server Topology" on the previous page](#).

For user interface details, see BSM Integration Data and Topology Settings in the Using SiteScope Guide.

# UI Descriptions

## Microsoft IIS Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of 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></p> <ul style="list-style-type: none"><li>• Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li><li>• When working in template mode, 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></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Counters</b>	<p>Displays 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>

UI Element	Description
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a> .

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<ul style="list-style-type: none"> <li>• Web Service – Anonymous Users/sec</li> <li>• Web Service – Bytes Received/sec</li> <li>• Web Service – Bytes Sent/sec</li> <li>• Web Service – Bytes Total/sec</li> <li>• Web Service – CGI Requests/sec</li> <li>• Web Service – Connection Attempts/sec</li> <li>• Web Service – Copy Requests/sec</li> <li>• Web Service – Current Anonymous Users</li> <li>• Web Service – Current Blocked Async I/O Requests</li> <li>• Web Service – Current CAL count for authenticated users</li> <li>• Web Service – Current CAL count for SSL connections</li> <li>• Web Service – Current CGI Requests</li> <li>• Web Service – Current Connections</li> <li>• Web Service – Current ISAPI Extension Requests</li> <li>• Web Service – Current NonAnonymous Users</li> <li>• Web Service – Delete Requests/sec</li> <li>• Web Service – Files Received/sec</li> <li>• Web Service – Files Sent/sec</li> <li>• Web Service – Files/sec</li> <li>• Web Service – Get Requests/sec</li> <li>• Web Service – Head Requests/sec</li> <li>• Web Service – ISAPI Extension Requests/sec</li> <li>• Web Service – Lock Requests/sec</li> <li>• Web Service – Locked Errors/sec</li> <li>• Web Service – Logon Attempts/sec</li> <li>• Web Service – Maximum Anonymous Users</li> <li>• Web Service – Maximum CAL count for authenticated users</li> </ul>	<ul style="list-style-type: none"> <li>• Web Service – Maximum CAL count for SSL connections</li> <li>• Web Service – Maximum CGI Requests</li> <li>• Web Service – Maximum Connections</li> <li>• Web Service – Maximum ISAPI Extension Requests</li> <li>• Web Service – Maximum NonAnonymous Users</li> <li>• Web Service – Measured Async I/O Bandwidth Usage</li> <li>• Web Service – Mkol Requests/sec</li> <li>• Web Service – Move Requests/sec</li> <li>• Web Service – NonAnonymous Users/sec</li> <li>• Web Service – Not Found Errors/sec</li> <li>• Web Service – Options Requests/sec</li> <li>• Web Service – Other Request Methods/sec</li> <li>• Web Service – Post Requests/sec</li> <li>• Web Service – Propfind Requests/sec</li> <li>• Web Service – Proppatch Requests/sec</li> <li>• Web Service – Put Requests/sec</li> <li>• Web Service – Search Requests/sec</li> <li>• Web Service – Service Uptime</li> <li>• Web Service – Total Allowed Async I/O Requests</li> <li>• Web Service – Total Anonymous Users</li> <li>• Web Service – Total Blocked Async I/O Requests</li> <li>• Web Service – Total CGI Requests</li> <li>• Web Service – Total Connection Attempts (all instances)</li> <li>• Web Service – Total Copy Requests</li> <li>• Web Service – Total count of failed CAL requests for authenticated users</li> <li>• Web Service – Total count of failed CAL requests for SSL connections</li> <li>• Web Service – Total Delete Requests</li> <li>• Web Service – Total Files Received</li> <li>• Web Service – Total Files Sent</li> <li>• Web Service – Total Files Transferred</li> <li>• Web Service – Total Get Requests</li> <li>• Web Service – Total Head Requests</li> </ul>	<ul style="list-style-type: none"> <li>• Web Service – Total ISAPI Extension Requests</li> <li>• Web Service – Total Lock Requests</li> <li>• Web Service – Total Locked Errors</li> <li>• Web Service – Total Logon Attempts</li> <li>• Web Service – Total Method Requests</li> <li>• Web Service – Total Method Requests/sec</li> <li>• Web Service – Total Mkol Requests</li> <li>• Web Service – Total Move Requests</li> <li>• Web Service – Total NonAnonymous Users</li> <li>• Web Service – Total Not Found Errors</li> <li>• Web Service – Total Options Requests</li> <li>• Web Service – Total Other Request Methods</li> <li>• Web Service – Total Post Requests</li> <li>• Web Service – Total Propfind Requests</li> <li>• Web Service – Total Proppatch Requests</li> <li>• Web Service – Total Put Requests</li> <li>• Web Service – Total Rejected Async I/O Requests</li> <li>• Web Service – Total Search Requests</li> <li>• Web Service – Total Trace Requests</li> <li>• Web Service – Total Unlock Requests</li> <li>• Web Service – Trace Requests/sec</li> <li>• Web Service – Unlock Requests/sec</li> </ul>
---	--	---

## Tips/Troubleshooting

### General General Notes/Limitations

- When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the **Browse Servers** and **Add Remote Server** buttons are not displayed.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify**

**monitor properties with remote server** check box in the Deployment Values dialog box.

## Troubleshooting and Limitations

- 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.

# Chapter 61: Microsoft Lync Server 2010 Monitors

Microsoft Lync Server 2010 monitors enable you to monitor performance, availability, and capacity planning on Microsoft A/V Conferencing Server, Microsoft Archiving Server, Microsoft Director Server, Microsoft Edge Server, Microsoft Front End Server, Microsoft Mediation Server, Microsoft Monitoring and CDR Server, and Microsoft Registrar Server.

You can monitor multiple parameters or counters on a single, remote server with each monitor instance. Create one or more Microsoft Lync Server 2010 monitor instances for each remote server in your environment. The error and warning thresholds for the monitor can be set on one or more performance statistics.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of Microsoft Lync server monitoring. For details, see Microsoft Lync Server 2010 Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the required Microsoft Lync Server 2010 monitor.

## Learn About

This section includes:

- ["Microsoft Lync Server 2010 Monitor Overview" below](#)
- ["Supported Platforms/Versions" on page 434](#)
- ["Support for IPv6 Addresses" on page 434](#)
- ["Server-Centric Report" on page 435](#)
- ["Configuring the Monitor to Run on Windows 2008 R2 as a Non-Administrator User" on page 435](#)
- ["License Consumption" on page 435](#)

## Microsoft Lync Server 2010 Monitor Overview

Use the Microsoft Lync Server 2010 monitors to watch server loading for performance, availability, and capacity planning on the following:

- **Microsoft A/V Conferencing Server.** Monitors the server performance statistics of the Microsoft Lync A/V Conferencing Server. A/V conferencing, enables real-time audio and video A/V communications between your users (that is, provided they have appropriate client devices such as headsets for audio conferences, and web cams for video conferences). A/V Conferencing Server provides A/V conferencing functionality to your deployment. It can be collocated with Front End Server, or deployed separately as a single server or A/V Conferencing Server pool.
- **Microsoft Archiving Server.** Monitors the server performance statistics of the Microsoft Lync Archiving Server. The Archiving Server enables you to archive instant messaging (IM) communications and meeting content for compliance reasons. Corporations and other organizations are subject to an increasing number of industry and government regulations that require the retention of specific types of communications.



With the Archiving Server feature, Microsoft Lync Server 2010 communications software provides a way for you to archive IM content, conferencing (meeting) content, or both that is sent through Lync Server 2010. If you deploy Archiving Server and associate it with Front End pools, you can set it to archive instant messages and conferences and specify the users for which archiving is enabled.

- **Microsoft Director Server.** Monitors the server performance statistics of the Microsoft Lync Director Server. A Director is a server running Microsoft Lync Server communications software that authenticates user requests, but does not home any user accounts or provide presence or conferencing services. Directors are most useful in deployments that enable external user access, where the Director can authenticate requests before sending them on to internal servers. Directors can also improve performance in organizations with multiple Front End pools.
- **Microsoft Edge Server.** Monitors the server performance statistics of the Microsoft Lync Edge Server. The Edge Server enables your users to communicate and collaborate with users outside the organization's firewalls. These external users can include the organization's own users who are currently working offsite, users from federated partner organizations, and outside users who have been invited to join conferences hosted on your Lync Server deployment. Edge Server also enables connectivity to public IM connectivity services, including Windows Live, AOL, and Yahoo!.
- **Microsoft Front End Server.** Monitors the server performance statistics of the Microsoft Lync Front End Server. The Front End Server is the core server role, and runs many basic Lync Server functions. The Front End Server, along with the Back End Servers, which provide the database, are the only server roles required to be in any Lync Server Enterprise Edition deployment.

A Front End pool is a set of Front End Servers, configured identically, that work together to provide services for a common group of users. A pool provides scalability and failover capability your users.

Front End Server includes the following functionality:

- User authentication and registration
  - Presence information and contact card exchange
  - Address book services and distribution list expansion
  - IM functionality, including multiparty IM conferences
  - Web conferencing and application sharing (if deployed)
  - Application hosting services, for both applications included with Lync Server (for example, Conferencing Attendant and Response Group application) and third-party applications
  - Application services for application hosting and hosts applications (for example, Response Group application, and several others)
- **Microsoft Mediation Server.** Monitors the server performance statistics of the Microsoft Lync Mediation Server. The Mediation Server is a necessary component for implementing Enterprise Voice and dial-in conferencing. The Mediation Server translates signaling and, in some configurations, media between your internal Lync Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk. On the Lync Server side, Mediation Server listens on a single mutual TLS (MTLS) transport address. On the gateway side, Mediation Server listens on a single TCP and single TLS transport address or a single TLS transport address. All qualified gateways must support TLS, but can enable TCP as well.
  - **Microsoft Monitoring and CDR Server.** Monitors the server performance statistics of the Microsoft Lync Monitoring and CDR Server. The Monitoring Server collects data about the quality of your network

media, in both Enterprise Voice calls and A/V conferences. This information can help you provide the best possible media experience for your users. It also collects call error records (CERs), which you can use to troubleshoot failed calls. Additionally, it collects usage information in the form of call detail records (CDRs) about various Lync Server features, so that you can calculate return on investment of your deployment, and plan the future growth of your deployment.

- **Microsoft Registrar Server.** Monitors the server performance statistics of the Microsoft Lync Registrar Server. The Lync Server 2010 Registrar is a new server role that enables client registration and authentication and provides routing services. It resides along with other components on a Standard Edition Server, Enterprise Front End Server, Director, or Survivable Branch Appliance. A Registrar pool consists of Registrar Services running on the Lync Server pool and residing at the same site.

## Supported Platforms/Versions

- This monitor supports monitoring Microsoft Lync Server 2010 servers.
- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

## Support for IPv6 Addresses

These monitors support the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the following protocols are supported:

- WMI (from SiteScope installed on Windows platforms only)
- NetBIOS (from SiteScope installed on Windows platforms only)

### Note:

- When using the **Direct registry queries** collection method with a NetBIOS connection, counters are not displayed in the Available Counters table. However, you can still use monitoring process if you modify the counters using the IPv4 protocol, or copy the counters from an already configured monitor (copy the monitor), and then change back to the IPv6 address or host.
- When using the **Microsoft Windows PDH Library** collection method with a NetBIOS connection, IPv6 does not work if the name of the monitored server is specified as a literal IPv6 address.
- When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## 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 Lync Server 2010 monitor in the SiteScope Dashboard. For details, see Creating Server-Centric Reports in the Using SiteScope Guide.

## Configuring the Monitor to Run on Windows 2008 R2 as a Non-Administrator User

For the Microsoft Lync Server 2010 monitors to monitor a Windows 2008 R2 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 ["How to Configure the Microsoft Lync Server 2010 Monitor" below](#).

## License Consumption

Points-based Usage	Capacity-based Usage
106 points for one instance of each Lync Server role.  (Additional points are used when deploying subtemplates for different machines with the same role.)	One OSi license per monitored host  Note: This monitor is not available when using Community edition.

# Tasks

## How to Configure the Microsoft Lync Server 2010 Monitor

### 1. Prerequisites

SiteScopes running on Windows platforms need 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.

For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

### 2. 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).

### 3. Configure user account settings on the remote monitored machine

The user account settings on the monitored remote 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 that 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]
```

**Note:** 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.

### 4. 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.

## 5. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## Microsoft Lync Server 2010 Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of the server where the Microsoft Lync Server 2010 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></p> <ul style="list-style-type: none"><li>• Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li><li>• When working in template mode, 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></ul> <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) Name of any SiteScope remote server from which you want to get counters (it must be accessible in the domain using NETBIOS). 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>

UI Element	Description
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 Serverslist 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Collection method</b>	<p>Select the collection method option. The Available Counters list is dynamically updated according to the collection method selected. This enables you to see the counters when creating or editing the monitor instead of when running the monitor:</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 <b>Default collection method for Microsoft Windows Resources monitor</b> in <b>Preferences &gt; Infrastructure Preferences &gt; General Settings</b>. The default value for this setting is PDH.</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>Enables collecting data specifically for generating the Server-Centric Report. The report displays various measurements for the server being monitored. For details, see Creating Server-Centric Reports in the Using SiteScope Guide.</p>
<b>Available Counters</b>	<p>Displays the available measurements for this monitor. For the list of counters that can be configured for the Microsoft Lync monitors, see <a href="#">"Monitor Counters" on page 440</a>.</p> <p>For each measurement, select the <b>Object</b>, <b>Instances</b> and <b>Counters</b> you want to check with the 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 the Microsoft Lync 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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for the Microsoft Lync monitors:

Monitor Type	Counters
Microsoft Archiving Server	<p><b>Archiving Server - Process Memory statistics monitoring policy</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>Archiving Server - Process CPU statistics monitoring policy</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Director Server - Process Memory statistics monitoring policy</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>Director Server - Process CPU statistics monitoring policy</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Replicator - Process Memory statistics monitoring policy</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>Replicator Server - Process CPU statistics monitoring policy</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul>
Microsoft A/V Conferencing Server	<p><b>A/V Server - Process Memory statistics monitoring policy</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>A/V Server - Process CPU statistics monitoring policy</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul>



Monitor Type	Counters
Microsoft Director Server	<b>Director Server - Process Memory statistics monitoring policy</b> <ul style="list-style-type: none"><li>• Working Set</li><li>• Private Bytes</li><li>• Page Faults/sec</li></ul> <b>Director Server - Process CPU statistics monitoring policy</b> <ul style="list-style-type: none"><li>• % Processor Time</li><li>• Thread Count</li></ul> <b>Replicator - Process Memory statistics monitoring policy</b> <ul style="list-style-type: none"><li>• Working Set</li><li>• Private Bytes</li><li>• Page Faults/sec</li></ul> <b>Replicator Server - Process CPU statistics monitoring policy</b> <ul style="list-style-type: none"><li>• % Processor Time</li><li>• Thread Count</li></ul>

Monitor Type	Counters
Microsoft Edge Server	<p><b>Audio/Video authentication Service - Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Audio/Video authentication Service - Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>Audio/Video Conferencing Service - Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Audio/Video Conferencing service (group) – Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>Access Edge service (group) – Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Access Edge service (group) – Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>WebConferencing edge service (group) – Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Web conferencing edge service (group) – Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul>

Monitor Type	Counters
Microsoft Front End Server	<p><b>Front End server - Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Front End server - Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>WebConferencing server - Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Web conferencing server - Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>IM Conferencing server - Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>IM Conferencing server - Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul>
Microsoft Mediation Server	<p><b>Mediation Server - Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Mediation server - Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul>

Monitor Type	Counters
Microsoft Monitoring Server	<p><b>CDR - Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>CDR - Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>Monitoring Server - Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Monitoring Server (group) – Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>Replicator (group) – Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Replicator (group) – Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul>
Microsoft Registrar Server	<p><b>Registrar Server (group) – Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Registrar server (group) – Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul> <p><b>Replicator Server (group) – Process CPU statistics</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> <li>• Thread Count</li> </ul> <p><b>Replicator server (group) – Process Memory statistics</b></p> <ul style="list-style-type: none"> <li>• Working Set</li> <li>• Private Bytes</li> <li>• Page Faults/sec</li> </ul>

## Tips/Troubleshooting

### General Notes/Tips

- When configuring these monitors in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

### Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Microsoft Lync Server 2010 monitors.

- Getting invalid CPU value error message in **<SiteScope root directory>\logs\RunMonitor.log** file when using perfmon monitors on VMware host servers. **Workaround:** Use the VMWare Performance monitor to measure CPU on VMWare host servers.
- If you encounter "Error: Object Processor not found on host" or "Error: Failed to collect the data" when running the Microsoft Lync Server 2010 monitors, change the collection method to the **Direct registry queries method** option.

# Chapter 62: Microsoft SQL Server Monitor

Use the Microsoft SQL Server monitor to monitor the server performance metrics pages for SQL 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 monitor instance for each Microsoft SQL Server you are running. The error and warning thresholds for the monitor can be set on one or more SQL Server performance statistics.

**Tip:** 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 Server 2005, 2008, and 2008 R2. For details, see Microsoft SQL Server Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft SQL Server monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["Microsoft SQL Server Topology" on the next page](#)
- ["License Consumption" on the next page](#)

## Supported Platforms/Versions

- The Microsoft SQL Server monitor supports monitoring Microsoft SQL Server versions 6.5, 7.1, 2000, 2005, 2008, 2008 R2, 2012, and 2014.
- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

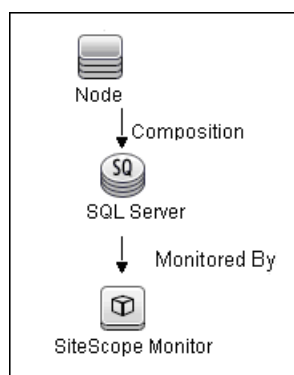
For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## Microsoft SQL Server Topology

The Microsoft SQL Server monitor can identify the topology of the Microsoft SQL Servers being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

# Tasks

## How to Configure the Microsoft SQL Server Monitor

1. Prerequisites
  - Make sure you have the specific access permissions required for this monitor as specified in Permissions and Credentials.
  - The Microsoft SQL Server monitor uses performance counters to measure application server performance. SiteScopes running on Windows platforms need 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. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "[Microsoft SQL Server Topology](#)" on the previous page.

For user interface details, see BSM Integration Data and Topology Settings in the Using SiteScope Guide.

## UI Descriptions

### Microsoft SQL Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of 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></p> <ul style="list-style-type: none"><li>Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li><li>When working in template mode, 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></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>



UI Element	Description
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 <a href="#">How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide</a>.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see <a href="#">New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide</a>.</p>
<b>SQL instance name</b>	<p>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>Displays 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>
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see [Common Monitor Settings in the Using SiteScope Guide](#).

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<p><b>SQLServer:Access Methods</b></p> <ul style="list-style-type: none"> <li>• AU cleanup batches/sec</li> <li>• AU cleanups/sec</li> <li>• By-reference Lob Create Count</li> <li>• By-reference Lob Use Count</li> <li>• Count Lob Readahead</li> <li>• Count Pull In Row</li> <li>• Count Push Off Row</li> <li>• Deferred dropped AUs</li> <li>• Deferred Dropped rowsets</li> <li>• Dropped rowset cleanups/sec</li> <li>• Dropped rowsets skipped/sec</li> <li>• Extent Deallocations/sec</li> <li>• Extents Allocated/sec</li> <li>• Forwarded Records/sec</li> <li>• FreeSpace Page Fetches/sec</li> <li>• FreeSpace Scans/sec</li> <li>• Full Scans/sec</li> <li>• Index Searches/sec</li> <li>• LobHandle Destroy Count</li> <li>• LobSS Provider Create Count</li> <li>• LobSS Provider Destroy Count</li> <li>• LobSS Provider Truncation Count</li> <li>• Mixed page allocations/sec</li> <li>• Page Deallocations/sec</li> <li>• Page Splits/sec</li> <li>• Pages Allocated/sec</li> <li>• Probe Scans/sec</li> <li>• Range Scans/</li> <li>• Scan Point Revalidations</li> <li>• Skipped Ghosted Records/sec</li> <li>• Table Lock Escalations/sec • Shrink Data Movement Bytes/sec</li> <li>• Transactions/sec</li> <li>• Used leaf page cookie</li> <li>• Used tree page cookie</li> <li>• Workfiles Created/sec</li> <li>• Worktables Created/sec</li> <li>• Worktables From Cache Ratio</li> </ul>	<p><b>SQLServer:Backup Device</b></p> <ul style="list-style-type: none"> <li>• Device Throughput Bytes/sec</li> </ul> <p><b>SQLServer:Buffer Manager</b></p> <ul style="list-style-type: none"> <li>• AWE lookup maps/sec</li> <li>• AWE stolen maps/sec</li> <li>• AWE unmap calls/sec</li> <li>• AWE unmap pages/sec</li> <li>• AWE write maps/sec</li> <li>• Buffer cache hit ratio</li> <li>• Checkpoint pages/sec</li> <li>• Database pages</li> <li>• Free list stalls/sec</li> <li>• Free pages</li> <li>• Lazy writes/sec</li> <li>• Page life expectancy</li> <li>• Page lookups/sec</li> <li>• Page reads/sec</li> <li>• Page writes/sec</li> <li>• Readahead pages/sec</li> <li>• Reserved pages</li> <li>• Stolen pages</li> <li>• Target pages</li> <li>• Total pages</li> </ul> <p><b>SQLServer:Buffer Partition</b></p> <ul style="list-style-type: none"> <li>• Free list empty/sec -- 0</li> <li>• Free list empty/sec -- 1</li> <li>• Free list requests/sec -- 0</li> <li>• Free list requests/sec -- 1</li> <li>• Free pages -- 0</li> <li>• Free pages -- 1</li> </ul> <p><b>SQLServer:CLR</b></p> <ul style="list-style-type: none"> <li>• CLR Execution</li> </ul>	<p><b>SQLServer:Cursor Manager by Type</b> (<b>_Total/API Cursor/TSQL Global Cursor/TSQL Local Cursor</b>)</p> <ul style="list-style-type: none"> <li>• Active cursors</li> <li>• Cache Hit Ratio</li> <li>• Cached Cursor Counts</li> <li>• Cursor Cache Use Counts/sec</li> <li>• Cursor memory usage</li> <li>• Cursor Requests/sec</li> <li>• Cursor worktable usage</li> <li>• Number of active cursor plans</li> </ul> <p><b>SQLServer:Cursor Manager Total</b></p> <ul style="list-style-type: none"> <li>• Async population count</li> <li>• Cursor conversion rate</li> <li>• Cursor flushes</li> </ul> <p><b>SQLServer:Database Mirroring</b></p> <ul style="list-style-type: none"> <li>• Bytes Received/sec</li> <li>• Bytes Sent/sec</li> <li>• Log Bytes Received/sec</li> <li>• Log Bytes Sent/sec</li> <li>• Log Send Queue KB</li> <li>• Pages Sent/sec</li> <li>• Receives/sec</li> <li>• Redo Bytes/sec</li> <li>• Redo Queue KB</li> <li>• Send/Receive Ack Time</li> <li>• Sends/sec</li> <li>• Transaction Delay</li> </ul> <p><b>SQLServer:Databases</b> (<b>_Total/&lt;per database&gt;</b>)</p> <ul style="list-style-type: none"> <li>• Active Transactions</li> <li>• Backup/Restore Throughput/sec</li> <li>• Bulk Copy Rows/sec</li> <li>• Bulk Copy Throughput/sec</li> <li>• Data File(s) Size (KB)</li> <li>• DBCC Logical Scan Bytes/sec</li> <li>• Log Bytes Flushed/sec</li> <li>• Log Cache Hit Ratio</li> <li>• Log Cache Reads/sec</li> </ul>
--	---	---

<ul style="list-style-type: none"> <li>• Log File(s) Size (KB)</li> <li>• Log File(s) Used Size (KB)</li> <li>• Log Flush Wait Time</li> <li>• Log Flush Waits/sec</li> <li>• Log Flushes/sec</li> <li>• Log Growths</li> <li>• Log Shrinks</li> <li>• Log Truncations</li> <li>• Percent Log Used</li> <li>• Repl. Pending Xacts</li> <li>• Repl. Trans. Rate</li> <li>• Shrink Data Movement Bytes/sec</li> <li>• Transactions/sec</li> </ul> <p><b>SQLServer:Exec Statistics</b> (Average execution time (ms)/Cumulative execution time (ms) per second/Execs in progress/Execs started per second)</p> <ul style="list-style-type: none"> <li>• Distributed Query</li> <li>• DTC calls</li> <li>• Extended Procedures</li> <li>• OLEDB calls</li> </ul> <p><b>SQLServer:General Statistics</b></p> <ul style="list-style-type: none"> <li>• Active Temp Tables</li> <li>• Event Notifications Delayed Drop</li> <li>• HTTP Authenticated Requests</li> <li>• Logical Connections</li> <li>• Logins/sec</li> <li>• Logouts/sec</li> <li>• Mars Deadlocks</li> <li>• Non-atomic yield rate</li> <li>• Processes blocked</li> <li>• SOAP Empty Requests</li> <li>• SOAP Method Invocations</li> <li>• SOAP Session Initiate Requests</li> <li>• SOAP Session Terminate Requests</li> <li>• SOAP SQL Requests</li> <li>• SOAP WSDL Requests</li> <li>• SQL Trace IO Provider Lock Waits</li> <li>• Temp Tables Creation Rate</li> <li>• Temp Tables For Destruction</li> <li>• Trace Event Notification Queue</li> <li>• Transactions</li> <li>• User Connections</li> </ul> <p><b>SQLServer:Latches</b></p> <ul style="list-style-type: none"> <li>• Average Latch Wait Time (ms)</li> <li>• Latch Waits/sec</li> <li>• Number of SuperLatches</li> <li>• SuperLatch Demotions/sec</li> <li>• SuperLatch Promotions/sec• Total Latch Wait Time (ms)</li> </ul>	<p><b>SQLServer:Locks</b> (_Total/AllocUnit/Application/Database/Extent/File/HoBT/Key/Metadata/Object/Page/RID)</p> <ul style="list-style-type: none"> <li>• Average Wait Time (ms) -- _Total</li> <li>• Average Wait Time (ms) -- Database</li> <li>• Average Wait Time (ms) -- Extent</li> <li>• Average Wait Time (ms) -- Key</li> <li>• Average Wait Time (ms) -- Page</li> <li>• Average Wait Time (ms) -- RID</li> <li>• Average Wait Time (ms) -- Table</li> <li>• Lock Requests/sec -- _Total</li> <li>• Lock Requests/sec -- Database</li> <li>• Lock Requests/sec -- Extent</li> <li>• Lock Requests/sec -- Key</li> <li>• Lock Requests/sec -- Page</li> <li>• Lock Requests/sec -- RID</li> <li>• Lock Requests/sec -- Table</li> <li>• Lock Timeouts/sec -- _Total</li> <li>• Lock Timeouts/sec -- Database</li> <li>• Lock Timeouts/sec -- Extent</li> <li>• Lock Timeouts/sec -- Key</li> <li>• Lock Timeouts/sec -- Page</li> <li>• Lock Timeouts/sec -- RID</li> <li>• Lock Timeouts/sec -- Table</li> <li>• Lock Wait Time (ms) -- _Total</li> <li>• Lock Wait Time (ms) -- Database</li> <li>• Lock Wait Time (ms) -- Extent</li> <li>• Lock Wait Time (ms) --</li> </ul>	<ul style="list-style-type: none"> <li>• Lock Wait Time (ms) -- Page</li> <li>• Lock Wait Time (ms) -- RID</li> <li>• Lock Wait Time (ms) -- Table</li> <li>• Lock Waits/sec -- _Total</li> <li>• Lock Waits/sec -- Database</li> <li>• Lock Waits/sec -- Extent</li> <li>• Lock Waits/sec -- Key</li> <li>• Lock Waits/sec -- Page</li> <li>• Lock Waits/sec -- RID</li> <li>• Lock Waits/sec -- Table</li> <li>• Number of Deadlocks/sec -- _Total</li> <li>• Number of Deadlocks/sec -- Database</li> <li>• Number of Deadlocks/sec -- Extent</li> <li>• Number of Deadlocks/sec -- Key</li> <li>• Number of Deadlocks/sec -- Page</li> <li>• Number of Deadlocks/sec -- RID</li> <li>• Number of Deadlocks/sec -- Table</li> </ul> <p><b>SQLServer:Memory Manager</b></p> <ul style="list-style-type: none"> <li>• Connection Memory (KB)</li> <li>• Granted Workspace Memory (KB)</li> <li>• Lock Blocks</li> <li>• Lock Blocks Allocated</li> <li>• Lock Memory (KB)</li> <li>• Lock Owner Blocks</li> <li>• Lock Owner Blocks Allocated</li> <li>• Maximum Workspace Memory (KB)</li> <li>• Memory Grants Outstanding</li> <li>• Memory Grants Pending</li> <li>• Optimizer Memory (KB)</li> <li>• SQL Cache Memory (KB)</li> <li>• Target Server Memory(KB)</li> <li>• Total Server Memory (KB)</li> </ul> <p><b>SQLServer:Plan Cache</b> (_Total/Bound Trees/Extended Stored Procedures/Object Plans/SQL Plans/Temporary Tables &amp; Table Variables)</p> <ul style="list-style-type: none"> <li>• Cache Hit Ratio</li> <li>• Cache Object Counts</li> <li>• Cache Objects in use</li> <li>• Cache Pages</li> </ul> <p><b>SQLServer:Replication</b></p> <ul style="list-style-type: none"> <li>• Agents Running</li> <li>• Dist</li> <li>• Logreader</li> <li>• Snapshot</li> </ul>
---	--	---

	Key	
<b>SQLServer:SQL Errors (_Total/DB Offline Errors/Info Errors/Kill Connection Errors/User Errors)</b> <ul style="list-style-type: none"> <li>• Errors/sec SQLServer:SQL Statistics</li> <li>• Auto-Param Attempts/sec</li> <li>• Batch Requests/sec</li> <li>• Failed Auto-Params/sec</li> <li>• Forced Parameterizations/sec</li> <li>• Safe Auto-Params/sec</li> <li>• SQL Attention rate</li> <li>• SQL Compilations/sec</li> <li>• SQL Re-Compilations/sec</li> <li>• Unsafe Auto-Params/sec</li> </ul>	<b>SQLServer:Transactions</b> <ul style="list-style-type: none"> <li>• Free Space in tempdb (KB)</li> <li>• Longest Transaction Running Time</li> <li>• NonSnapshot Version Transactions</li> <li>• Snapshot Transactions</li> <li>• Transactions</li> <li>• Update conflict ratio</li> <li>• Update Snapshot Transactions</li> <li>• Version Cleanup rate (KB/s)</li> <li>• Version Generation rate (KB/s)</li> <li>• Version Store Size (KB)</li> <li>• Version Store unit count</li> <li>• Version Store unit creation</li> <li>• Version Store unit truncation</li> </ul>	<b>SQLServer:User Settable (User counter 1/User counter 2/User counter 3/User counter 4/ User counter 5/User counter 6/User counter 7/User counter 8/User counter 9/User counter 10)</b> <ul style="list-style-type: none"> <li>• Query</li> </ul> <b>SQLServer:Wait Statistics (Average wait time (ms)/Cumulative wait time (ms) per second/Waits in progress/Waits started per second)</b> <ul style="list-style-type: none"> <li>• Lock waits</li> <li>• Log buffer waits</li> <li>• Log write waits</li> <li>• Memory grant queue waits</li> <li>• Network IO waits</li> <li>• Non-Page latch waits</li> <li>• Page IO latch waits</li> <li>• Page latch waits</li> <li>• Thread-safe memory objects waits</li> <li>• Transaction ownership waits</li> <li>• Wait for the worker</li> <li>• Workspace synchronization waits</li> </ul>

## Tips/Troubleshooting

### General Notes/Tips

- When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the **Browse Servers** and **Add Remote Server** buttons are not displayed.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

### Troubleshooting and Limitations

**Problem:** SiteScope is unable to retrieve instances and counters from a Microsoft SQL Server 2008 when using the WMI connection method.

**Solution:**

1. Configure the monitor to use the NetBIOS connection.
2. If this does not work, you can monitor Microsoft SQL Server 2008 using the Microsoft Windows Resources monitor.

# Chapter 63: Microsoft Windows Dial-up Monitor (Deprecated)

**Note:** The Microsoft Windows Dial-up monitor was deprecated, and is currently not planned for future versions of SiteScope. If this monitor was configured in a previous version of SiteScope, it will still work after performing a SiteScope upgrade (but we do not recommend using it). This monitor is supported in SiteScope 11.24 and earlier versions.

The Microsoft Windows Dial-up monitor uses the Windows 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.

**Note:**

- This monitor requires an Operating System Instance (OSi) license with sufficient available capacity to create it in the SiteScope interface. For license purchase inquiries (or if you require additional capacity), contact your HPE sales representative or use the “Contact Us” link in the [HPE SiteScope Product page](#).
- Microsoft Windows Dial-up monitors consume one OS instance per 15 monitors.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Dial-up monitor.

## Learn About

This section includes:

- ["Microsoft Windows Dial-up Monitor Overview" below](#)
- ["Supported Platforms/Versions" on the next page](#)
- ["Status" on the next page](#)
- ["Scheduling the Monitor" on the next page](#)

## 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.

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 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.

## Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows versions only.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012.

## 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 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 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.

# Tasks

## How to Configure the Microsoft Windows Dial-up Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## Microsoft Windows Dial-up Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Account Settings</b>	

UI Element	Description
Phone number	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.
Account user name	Login name for the dial-up account.
Account password	Password for the dial-up account.
<b>Advanced Settings</b>	
Timeout (seconds)	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.  <b>Default value:</b> 60 seconds
<b>Monitor Settings</b>	
Monitor (s) to run	Groups, monitors, or both, that you want to run while the dial-up connection is established.  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.  Make sure that the Frequency box for these monitors is set to 0. For details, see Monitor Run Settings in the Using SiteScope Guide.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Tips

This monitor cannot be copied to a template. It must be created directly in a template.

### Troubleshooting and Limitations

This section describes troubleshooting and limitations 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.



# Chapter 64: Microsoft Windows Event Log Monitor

The Microsoft Windows Event Log monitor enables you to monitor the Microsoft Windows Event Logs (System, Application, or Security) for added entries.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Event Log monitor.

## Learn About

This section includes:

- ["Microsoft Windows Event Log Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Configuring SiteScope Alerts" below](#)
- ["Status" on the next page](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)
- ["License Consumption" on the next page](#)

## 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.

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see *SiteScope Monitoring Using Secure Shell (SSH)* in the *Using SiteScope Guide*.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see *Configure the WMI Service for Remote Monitoring* in the *Using SiteScope Guide*.

## 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.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor  Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

# Tasks

## How to Configure the Microsoft Windows Event Log Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor

as specified in Permissions and Credentials.

2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Tip:** The **Event Log Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Event Log Tool in the Using SiteScope Guide.

## UI Descriptions

### Microsoft Windows Event Log Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of 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:</b></p> <ul style="list-style-type: none"><li>• Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li><li>• When configuring this monitor on SiteScopes running on UNIX versions:<ul style="list-style-type: none"><li>• Only remote servers that have been configured with an <b>SSH</b> connection method and <b>SSH using preinstalled SiteScope remote Windows SSH files</b> is selected are displayed. For details, see How to Configure Remote Windows Servers for SSH monitoring.</li><li>• If you create a new remote server from the Monitor Settings panel, the <b>SSH using preinstalled SiteScope remote Windows SSH files</b> setting is automatically selected and cannot be cleared.</li><li>• When working in template mode, 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></ul></li></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>

UI Element	Description
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Log name</b>	<p>Select the event log to monitor. The list of event logs is automatically generated from the target server (from the registry for NetBIOS/SSH connections, and from WMI Classes for WMI connections).</p> <p><b>Note:</b> When using a NetBIOS or WMI connection, only the IDs (names) are displayed for independent libraries. For example, if you install Microsoft Office Diagnostics, only ODiag is displayed as the log name. To display the whole name, manually add the log name to the <b>event_log_names.properties</b> file in &lt;SiteScope root directory&gt;\template.applications.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• ODiag=Microsoft Office Diagnostics</li> <li>• OSession=Microsoft Office Sessions</li> <li>• HardwareEvents=Hardware Events</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• Only add names to <b>event_log_names.properties</b> that are different from the IDs, otherwise all names will be the same as IDs.</li> <li>• Logs are no longer automatically updated after opening the monitor's properties. Instead, click the <b>Reload Logs List</b> button to reload the selected logs.</li> </ul>
<b>Reload Logs List</b>	<p>Reload the selected logs.</p>

UI Element	Description
<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>• Audit Failure</li> <li>• Audit Success</li> <li>• Warning</li> <li>• Error or warning</li> <li>• Information</li> </ul>
<b>Run alerts</b>	<p>Method for running alerts:</p> <ul style="list-style-type: none"> <li>• <b>For each event matched.</b> The monitor triggers alerts for every matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error). For useful information, see <a href="#">"Configuring SiteScope Alerts" on page 457</a>.</li> <li>• <b>Once, after all events have been checked.</b> The monitor counts up the number of matches and triggers alerts based on the warning and error threshold settings.</li> </ul>
<b>Source and ID match</b>	<p>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>Event Source depends on the monitor connection method:</p> <ul style="list-style-type: none"> <li>• If WMI is used, Event Source equals Provider Name.</li> <li>• If NetBios is used and the event has no EventSourceName, Event Source equals Provider Name.</li> <li>• If NetBios is used and the event has an EventSourceName, Event Source equals Event Source Name.</li> </ul> <p><b>Examples:</b></p> <ul style="list-style-type: none"> <li>• <code>Print:20</code> matches event source named Print and event ID of 20.</li> <li>• To match against all events from a specific source, enter just the event source name. For example, <code>w3svc</code></li> <li>• To match an exact event ID from an event source, specify both. For example, <code>Service Control Mar:7000</code></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 in the Using SiteScope Guide.</p>

UI Element	Description
<b>Source and ID do not match</b>	<p>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 an event source named Print and event ID of 20 must not be in the event 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 in the Using SiteScope Guide.</p>
<b>Description match</b>	<p>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 in the Using SiteScope Guide.</p>
<b>Description does not match</b>	<p>Text string description that must not be in the event 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 in the Using SiteScope Guide.</p>
<b>Event category</b>	<p>Matches the category number of the event entry. Leaving this blank matches events with any category.</p>
<b>Event machine</b>	<p>Matches against the machine that added the entry to the log file. Leaving this blank matches events with any machine.</p>

UI Element	Description
<b>Interval (minutes)</b>	<p>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 Error If threshold to matches in interval <math>\geq 3</math>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and limitations for the Microsoft Windows Event Log monitor.

- ["General Notes/Tips" below](#)
- ["Monitor fails to get data from Windows remote servers with large amounts of log items when using a WMI connection" below](#)
- ["Unable to monitor custom event logs on a remote Microsoft Windows Server 2008" on the next page](#)

### General Notes/Tips

- If the Microsoft Windows Event Log monitor times out before reading all event log entries, it displays a message reflecting the number of skipped entries and a timeout value in the monitor summary string. You can force SiteScope to go back and re-read all events until all of them have been read on the next run (since it does not read the events that were unread on the previous run by default), by adding the `_fetchAllEventsFromStartAfterTimeout=true` property to the `<SiteScope root directory>\groups\master.config` file.
- When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the **Browse Servers** and **Add Remote Server** buttons are not displayed.
- To manage the behavior of the Microsoft Windows Event Log monitor, use the `_NTEventEmptyResultsCounter` property in `<SiteScope root directory>\groups\ master.config` to set the number of empty results after which the events counter will be reset to zero. The default value for this property is 1. This means that the events counter will be reset to zero if the monitor gets at least one empty result. If you want to disable the events counter reset option, set the property value to 0 or a minus number. This option is available only for a Microsoft Windows Event Log monitor which uses a WMI connection method.

### Monitor fails to get data from Windows remote servers with large amounts of log items when using a WMI connection

If the Microsoft Event Log monitor fails to get data from Windows remote servers with large amounts of log items when using the WMI connection type, change the query hour range of the first monitor run in the **Microsoft Windows Event Log monitor WMI query hour range in first run** box in **Preferences > Infrastructure Preferences > Custom Settings**. The default query range is the last 168 hours (7 days).

## Unable to monitor custom event logs on a remote Microsoft Windows Server 2008

To make a custom log file accessible:

1. Add the file to the registry.

For example, to monitor a custom event log called TaskScheduler (C:\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler\Operational.evtx), you must add a registry key **Microsoft-Windows-TaskScheduler/Operational** under **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\eventlog** on the remote machine.

2. After adding the registry key, you can see the log in the list of available log files by running the PowerShell “get-eventlog -list” command on the remote server:

```
PS C:\Users\Administrator> get-eventlog -list
```

Max(K)	Retain	OverflowAction	Entries	Log
20,480	0	OverwriteAsNeeded	162	Application
20,480	0	OverwriteAsNeeded	0	HardwareEvents
512	7	OverwriteOlder	0	Internet Explorer
20,480	0	OverwriteAsNeeded	0	Key Management Service
512	7	OverwriteOlder	162	<u>Microsoft-Windows-TaskScheduler/Operational</u>
20,480	0	OverwriteAsNeeded	304	Security
20,480	0	OverwriteAsNeeded	769	System
15,360	0	OverwriteAsNeeded	9	Windows PowerShell

3. The log is automatically displayed in the Microsoft Windows Event Log Monitor Settings:

Server: 172.24.151.110 [Browse Servers] [Add Remote Server]

Log name: Microsoft-Windows-TaskScheduler/Operational

Event type: Application

Run alerts: Internet Explorer

Source and ID match: Key Management Service

Source and ID do not match: Microsoft-Windows-TaskScheduler/Operational

Description match: Security

Description does not match: System

[Open Tool]

4. Configure the events to match in the log, and use SiteScope to monitor this log for events.



### Example

Matching an exact event ID (200) in the TaskScheduler log file:

Microsoft Windows Event Log Monitor Settings

Server: 172.24.151.110 [Browse Servers](#) [Add Remote Server](#)

Log name: Microsoft-Windows-Task Scheduler/Operational

Event type: Any

Run alerts: For each event matched

Source and ID match: Microsoft-Windows-Task Scheduler:200 [Open Tool](#)

Source and ID do not match:  [Open Tool](#)

Description match:  [Open Tool](#)

Description does not match:  [Open Tool](#)

Event category:

Event machine:

Interval (minutes): 0

# Chapter 65: Microsoft Windows Media Player Monitor (Deprecated)

**Note:** The Microsoft Windows Media Player monitor was deprecated, and is currently not planned for future versions of SiteScope. If this monitor was configured in a previous version of SiteScope, it is still displayed in SiteScope after performing an upgrade (but will not work). This monitor is supported in SiteScope 11.24 and earlier versions.

The Microsoft Windows Media Player monitor enables you to monitor availability and delivery quality parameters for media files and streaming data compatible with Windows Media Servers.

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. The error and warning thresholds for the monitor can be set on one or more Windows Media Player performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Media Player monitor.

## Learn About

### Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows versions only.
- This monitor supports monitoring Windows Media Player 7.x, 9.x, 10.x, 11.0, and 12.
- Monitor video streams only with this monitor (not audio streams).
- This monitor does not support the .asx or .mov formats.

## Tasks

### How to Configure the Microsoft Windows Media Player Monitor

#### 1. Prerequisites

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 ["Monitor Counters" on the next page](#).

#### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Microsoft Windows Media Player Monitor Settings

User interface elements are described below:

UI Element	Description
<b>URL</b>	<p>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> <code>mms://&lt;servername&gt;/sample.asf</code> for a unicast stream or <code>http://&lt;servername&gt;/stationid.nsc</code> 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>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>Media player performance parameters or counters to check with the Microsoft Windows Media Player monitor.</p> <p>For details on the available parameters or counters, see <a href="#">"Monitor Counters" below</a>.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

### Monitor Counters

Below is the list of counters that you can check with the Microsoft Windows Media Player monitor:

<b>Buffering count</b>	Number of times the Player had to buffer incoming media data due to insufficient media content.
<b>Buffering time</b>	Time spent waiting for sufficient media data to continue playing the media clip.
<b>Interrupts</b>	Number of interruptions encountered while playing a media clip. This includes buffering and playback errors.
<b>Packets lost</b>	Number of lost packets not recovered (applicable to network playback).
<b>Packets recovered</b>	Number of lost packets successfully recovered (applicable to network playback).
<b>Packet quality</b>	Percentage ratio of packets received to total packets.

<b>Ratio bandwidth</b>	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>	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>	Total duration of the media clip in seconds. This value is not effected by what was already played.
<b>Sampling rate</b>	Sampling rate in milliseconds, for collecting statistics.
<b>Stream count</b>	Packet count.
<b>Stream max</b>	Maximum number of packets.
<b>Stream min</b>	Minimum number of packets.
<b>Stream rate</b>	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>	Percentage of stream samples received on time (no delays in reception).

# Chapter 66: Microsoft Windows Media Server Monitor

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. The error and warning thresholds for the monitor can be set on one or more Windows Media server performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Media Server monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" on the next page](#)

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports all supported versions of Microsoft Windows Media Server through perfmon.  
**Note:** Windows Media Server is supported and maintained by Microsoft up to and including Windows Server 2008 R2 only.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSI license per monitored host

# Tasks

## How to Configure the Microsoft Windows Media Server Monitor

### 1. Prerequisites

- Make sure you have the specific access permissions required for this monitor as specified in Permissions and Credentials.
- The Microsoft Windows Media Server monitor uses performance counters to measure application server performance. SiteScopes running on Windows platforms need 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. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Note:** 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**.

## UI Descriptions

### Microsoft Windows Media Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of 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></p> <ul style="list-style-type: none"><li>• Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li><li>• When working in template mode, 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></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Counters</b>	<p>Displays 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>

UI Element	Description
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a> .

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<b>Windows Media Station Service</b> <ul style="list-style-type: none"><li>• Controllers</li><li>• Stations</li><li>• Streams</li></ul> <b>Windows Media Unicast Service</b> <ul style="list-style-type: none"><li>• Active Live Unicast Streams</li><li>• Active Streams</li><li>• Active TCP Streams</li><li>• Active UDP Streams</li><li>• Aggregate Read Rate</li><li>• Aggregate Send Rate</li><li>• Allocated Bandwidth</li><li>• Authentication Requests</li><li>• Authentications Denied</li><li>• Authorization Requests</li></ul>	<ul style="list-style-type: none"><li>• Authorizations Refused</li><li>• Connected Clients</li><li>• Connection Rate</li><li>• HTTP Streams</li><li>• HTTP Streams Reading Header</li><li>• HTTP Streams Streaming Body</li><li>• Late Reads</li><li>• Pending Connections</li><li>• Plugin Errors --</li><li>• Plugin Events</li><li>• Scheduling Rate</li><li>• Stream Errors</li><li>• Stream Terminations</li><li>• UDP Resend Requests</li><li>• UDP Resends Sent</li></ul>
---	--

## Tips/Troubleshooting

### General Notes/Tips

- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.



# Chapter 67: Microsoft Windows Performance Counter Monitor

The Microsoft Windows Performance Counter monitor enables you to track the values of any Windows performance statistic. These are the same statistics that can be viewed using the Microsoft Management Console under Windows.

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Performance Counter monitor.

## Learn About

### Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor Note: No points are consumed by this monitor if It is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

## Tasks

### How to Configure the Microsoft Windows Performance Counter Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Tip:** The **Performance Counters Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Performance Counters Tool in the Using SiteScope Guide.

## UI Descriptions

### Microsoft Windows Performance Counter Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of 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>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
<b>PerfMon chart file</b>	<p>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. The files in this list all reside in the <b>&lt;SiteScope root directory&gt;\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 <b>&lt;SiteScope root directory&gt;\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>	<p>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.</p>
<b>Counter</b>	<p>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.</p> <p>For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</p>
<b>Units</b>	<p>The units to be displayed with the counter's values to make them more readable.</p>
<b>Instance</b>	<p>The instance in the Microsoft Windows Performance monitor application. The instance name is case sensitive. Some counters can have multiple instances, for example, on machines with two CPUs, there are two instances of the Processor object. 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.</p>
<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: 1</b></p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<b>System</b> <ul style="list-style-type: none"><li>• % Total Processor Time</li><li>• File Data Operations/sec</li><li>• Processor Queue Length</li><li>• Total Interrupts/sec</li></ul> <b>Processor</b> <ul style="list-style-type: none"><li>• % Processor Time</li></ul> <b>Objects</b> <ul style="list-style-type: none"><li>• Threads</li></ul>	<b>Process</b> <ul style="list-style-type: none"><li>• Private Bytes</li></ul> <b>Physical Disk</b> <ul style="list-style-type: none"><li>• % Disk Time</li></ul> <b>Memory</b> <ul style="list-style-type: none"><li>• Page Faults/sec</li><li>• Pages/sec</li><li>• Pool Nonpaged Bytes</li></ul>
--	---

## Tips/Troubleshooting

### General Notes/Limitations

When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the **Browse Servers** and **Add Remote Server** buttons are not displayed.

# Chapter 68: Microsoft Windows Resources Monitor

The Microsoft Windows Resources monitor enables you to monitor system performance data on Windows systems. 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. The error and warning thresholds for the monitor can be set on one or more performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Resources monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["Support for IPv6 Addresses" below](#)
- ["Server-Centric Report" on the next page](#)
- ["Configuring the Monitor to Run on Windows 2003 as a Non-Administrator User" on the next page](#)
- ["License Consumption" on the next page](#)

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

## Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the following protocols are supported:

- WMI (from SiteScope installed on Windows platforms only)
- NetBIOS (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:**

- When using the **Direct registry queries** collection method with a NetBIOS connection, counters are not displayed in the Available Counters table. However, you can still use monitoring process if you modify the counters using the IPv4 protocol, or copy the counters from an already configured monitor (copy the monitor), and then change back to the IPv6 address or host.
- When using the **Microsoft Windows PDH Library** collection method with a NetBIOS connection, IPv6 does not work if the name of the monitored server is specified as a literal IPv6 address.
- When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## 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 the SiteScope Dashboard. For details, see Creating Server-Centric Reports in the Using SiteScope Guide.

## 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 ["How to Configure the Microsoft Windows Resources Monitor" on the next page](#).

## License Consumption

Points-based Usage	Capacity-based Usage
One point per instance Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

# Tasks

## How to Configure the Microsoft Windows Resources Monitor

### 1. Prerequisites

- Make sure you have the specific access permissions required for this monitor as specified in Permissions and Credentials.
- SiteScopes running on Windows platforms need 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. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

### 2. 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).

### 3. Configure user account settings on the remote monitored machine

The user account settings on the monitored remote 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]
```

**Note:** 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, select the user that 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.

#### 4. 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 can connect to the remote machine, the Performance object box is filled in with the performance objects that can be monitored from the remote machine.

#### 5. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.





## UI Descriptions

### Microsoft Windows Resources Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of the 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></p> <ul style="list-style-type: none"><li>• Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</li><li>• When configuring this monitor on SiteScopes running on UNIX versions, only remote servers that have been configured with an <b>SSH</b> connection method are displayed. For details, see How to Configure Remote Windows Servers for SSH monitoring.</li><li>• When working in template mode, 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></ul> <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) Name of any SiteScope remote server from which you want to get counters (it must be accessible in the domain using NETBIOS). 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>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
<b>Collection method</b>	<p>Select the collection method option. The Available Counters list is dynamically updated according to the collection method selected. This enables you to see the counters when creating or editing the monitor instead of when running the monitor:</p> <ul style="list-style-type: none"> <li>• <b>Microsoft Windows PDH Library</b> Uses the Windows PDH library which is the most common option.</li> <li>• <b>Use global setting.</b> Instructs the monitor to use the value configured in <b>Default collection method for Microsoft Windows Resources monitor</b> in <b>Preferences &gt; Infrastructure Preferences &gt; General Settings</b>. The default value for this setting is PDH. This is the default option.</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.</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>Enables collecting data specifically for generating the Server-Centric Report. The report displays various measurements for the server being monitored. For details, see <i>Creating Server-Centric Reports</i> in the <i>Using SiteScope Guide</i>.</p>
<b>Available Counters</b>	<p>Displays the available measurements for this monitor.</p> <p>For each measurement, select the <b>Objects</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> <p>For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</p> <p><b>Note:</b> Objects are no longer automatically updated after opening the monitor's properties. Instead, click the <b>Reload Objects</b> button to reload data for the selected objects.</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>
<b>Reload objects</b>	<p>Reloads data for the selected objects.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see *Common Monitor Settings* in the *Using SiteScope Guide*.

## Monitor Counters

You can monitor any Windows Performance Monitor (Perfmon) counters. Commonly monitored counters are listed below:

<p><b>System</b></p> <ul style="list-style-type: none"> <li>• % Total Processor Time</li> <li>• File Data Operations/sec</li> <li>• Processor Queue Length</li> <li>• Total Interrupts/sec</li> </ul> <p><b>Processor</b></p> <ul style="list-style-type: none"> <li>• % Processor Time</li> </ul> <p><b>Objects</b></p> <ul style="list-style-type: none"> <li>• Threads</li> </ul>	<p><b>Process</b></p> <ul style="list-style-type: none"> <li>• Private Bytes</li> </ul> <p><b>Physical Disk</b></p> <ul style="list-style-type: none"> <li>• % Disk Time</li> </ul> <p><b>Memory</b></p> <ul style="list-style-type: none"> <li>• Page Faults/sec</li> <li>• Pages/sec</li> <li>• Pool Nonpaged Bytes</li> </ul>
--	--

## Tips/Troubleshooting

### General Notes/Tips

- 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.
- When monitoring Windows servers configured using SSH, you must use the **Direct registry queries** option for the **Collection method**.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When configuring this monitor in template mode:
  - You can use regular expressions to define counters.
- The **Add Remote Server** button is not displayed.

### Troubleshooting and Limitations

- The Microsoft Windows Resources monitor is unable to display non-UTF characters in instance or counter names when the NetBIOS connection is used.
- Getting invalid CPU value error message in **<SiteScope root directory>\logs\RunMonitor.log** file when using perfmon monitors on VMware host servers. **Workaround:** Use the VMware Performance monitor to measure CPU on VMware host servers.
- If you encounter "Error: Object Processor not found on host" or "Error: Failed to collect the data" when running the Microsoft Windows Resources monitor, change the collection method to the **Direct registry queries method** option.
- If you encounter inconsistent data when configuring Microsoft Windows Resources monitors with many counters on a loaded network environment, you can specify a timeout value for the monitor (for example, 300 seconds) in **Preferences > Infrastructure Preferences > Monitor Settings > Perfex options**.

# Chapter 69: Microsoft Windows Services State Monitor

The Microsoft Windows Services State monitor enables you 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.

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Microsoft Windows Services State monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption " on the next page](#)

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

## Tasks

### How to Configure the Microsoft Windows Services State Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Microsoft Windows Services State Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>The name of the 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></p> <ul style="list-style-type: none"><li>• 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 <i>Configure the WMI Service for Remote Monitoring</i> in the <i>Using SiteScope Guide</i>.</li><li>• When configuring this monitor on SiteScopes running on UNIX versions:<ul style="list-style-type: none"><li>• Only remote servers that have been configured with an <b>SSH</b> connection method and <b>SSH using preinstalled SiteScope remote Windows SSH files</b> is selected are displayed. For details, see <i>How to Configure Remote Windows Servers for SSH monitoring</i>.</li><li>• If you create a new remote server from the Monitor Settings panel, the <b>SSH using preinstalled SiteScope remote Windows SSH files</b> setting is automatically selected and cannot be cleared.</li></ul></li><li>• When working in template mode, 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></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 <i>How to Configure SiteScope to Monitor a Remote Microsoft Windows Server</i> in the <i>Using SiteScope Guide</i>.</p>

UI Element	Description
<b>Add Remote Server</b>	Opens the Add New Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.
<b>Services to include</b>	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.  <b>Default value:</b> /(.*)/ (All of the services detected on the remote machine)  <b>Examples:</b> /. *Network.*/ includes all services that contain the word Network.
<b>Services to ignore</b>	Optional regular expression to filter the list of services matched by the expression used in the Services to include setting. When you use a Services to ignore regular expression to filter the list of Services to include, the monitor calculates changes in state (that is, running or not running) based only on the services matched by the Services to ignore regular expression.  Capabilities include monitoring services added, services changed to running/not running, services currently running/not running, services deleted, services last running, number of services added, number of services changed to not running, number of services currently running/not running, number of services deleted.  <b>Examples:</b> /. *Remote.*/ ignores all services that contain the word Remote (the services that are ignored are listed in the <b>Services Deleted</b> field).
<b>Include driver services</b>	Includes all low-level driver services in the monitor. This generally increases the size of the list. You use the Services to include and Service to ignore options to filter the list of services returned using this option.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- Services added
- Services changed to not running
- Services changed to running
- Services currently not running
- Services currently running
- Services deleted
- Services last running
- Number of services added
- Number changed to not running
- Number of services currently not running
- Number of services currently running
- Number of services deleted

## Tips/Troubleshooting

### General Notes/Limitations

- 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).
- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- 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.



# Chapter 70: Multi Log Monitor

The Multi Log monitor checks for specific entries added to log files in given log directories by looking for entries containing a text phrase or a regular expression.

To access

In a SiteScope configured with System Health, select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Multi Log monitor.

## Learn About

This section includes:

- ["Multi Log Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Support for IPv6 Addresses" below](#)
- ["License Consumption" on the next page](#)

### Multi Log Monitor Overview

The Multi Log monitor watches for specific entries added to multiple log files in given log directories 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 can change this default behavior using the **Search from start** setting.

### Supported Platforms/Versions

- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor also supports monitoring remote servers running on UNIX and HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see ["How to Configure the HP NonStop Resources Monitor" on page 307](#).

### Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the following protocols are supported:

- NetBIOS (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per file	One OSi license per monitored host

# Tasks

## How to Configure the Multi Log Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Note:** For reading log directories on remote Red Hat Linux machines, the **Disable connection caching** check box must be selected in the remote server's Advanced Settings, otherwise the Multi Log monitor will not work.

# UI Descriptions

## Multi Log Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	

UI Element	Description
<b>Server</b>	<p>Name of the server where the files you want to monitor are 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 Windows domain, you can use the UNC format to specify the path to the remote log directory. You can also use a local file system path, such as C:\logDir.</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>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p> <p><b>Note:</b> For reading log directories on remote Red Hat Linux machines, the <b>Disable connection caching</b> check box must be selected in the remote server's Advanced Settings, otherwise the Multi Log File monitor will not work.</p>

UI Element	Description
<b>Log file directories</b>	<p>Path to the log file directories you want to monitor. The monitor runs on all files in the directory. For example, C:\logDir for a Windows remote server, or /tmp/logDirs for a UNIX remote server.</p> <p>To monitor multiple directories, enter the log file directory names separated by a semi-colon (;). For example, C:\logdir1;C:\logdir2.</p> <p><b>For Windows remote servers:</b></p> <ul style="list-style-type: none"> <li>For reading log files using the NetBIOS method: <ul style="list-style-type: none"> <li>You can use UNC to specify the path to the remote log file directory, such as \\remoteserver\sharedfolder\logdir. You can also use a local file system path, such as C:\logDir.</li> <li>All ":" characters will automatically be replaced by "\$".</li> <li>There is no need to specify the full name of the host.</li> </ul> </li> <li>For reading log files using the SSH method, specify the local path of the remote log file on the remote machine. For example: C:\Windows\System32\logdir <b>Note:</b> On some SSH servers for Windows (such as Cygwin), the path might need to be specified in UNIX style. For example, /cygwin/C/logDir. 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</li> <li>You can also monitor files local to the server where SiteScope is running. For example C:\application\appLogs\logDir</li> </ul> <p><b>For UNIX remote servers:</b></p> <ul style="list-style-type: none"> <li>For reading log directories on remote UNIX machines, it is recommended to use the absolute path to the directory of the UNIX user account being used to log into the remote machine. For example, /etc or /tmp.</li> <li>UNIX remotes support bash patterns. Patterns only work if the path contains the asterisk character (*); otherwise, they will not be triggered. For example: /root/test* will recursively find all directories in dir /root/test/.</li> </ul> <p>Optionally, you can use special date and time regular expression variables to match folders and log file names that include date and time information. For details, see "Date/Time Regular Expression Variables" in the <b>File name match</b> description below.</p>

UI Element	Description
<b>File name match</b>	<p>File name to look for in the specified log directories. You must use a regular expression in this entry to match text patterns, otherwise a verification error will be shown. Note that this option matches the full file path (with parent directories).</p> <p><b>Date/Time Regular Expression Variables</b></p> <p>Optionally, you can use special date and time regular expression variables to match folders and log file names that include date and time information. For example, you can use a syntax of <code>s/ex\$shortYear\$\$month\$\$day\$.log/</code> to match a current date-coded log file. For details on using regular expressions, see SiteScopeBSM Connector Date Variables and Examples for Log File MonitoringPolicies in the Using SiteScope Guide.</p> <p>Examples for Windows remote servers:</p> <pre>s/c:\app\logs\\$year\$\\$monthName\$/;s/d:\app2\logs\\$year\$\\$monthName\$/ - Log files directories</pre> <pre>s/\$hour\$.log/ - File name match</pre> <p>Examples for UNIX remote servers:</p> <pre>s//opt/app/logs/\$year\$/\\$monthName\$/;s//opt/app2/logs/\$year\$/\\$monthName\$/ - Log files directories</pre> <pre>s/\$hour\$.log/ - File name match</pre>
<b>Content match</b>	<p>Text to match in the log entries. You must use a regular expression in this entry to match text patterns, otherwise a verification error will be shown.</p> <p>Unlike the content match function of other SiteScope monitors, the Multi 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 <code>s</code> search modifier to the end of the regular expression. For details, see Regular Expressions in the Using SiteScope Guide.</p> <p><b>Note:</b> There is a limit of 10 content match values. When creating a report by clicking the monitor title, the report includes only the first 10 values, if more than 10 were entered.</p>
<b>Match value labels</b>	<p>Use to enter labels for the matched values found in the target log directories. 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 (,).</p> <p>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 (not in Quick Reports) for this monitor. The order of labels is the same as the order of matches.</p> <p><b>Note:</b> When you create a report by clicking the monitor title, the report includes up to 10 match value labels.</p>

UI Element	Description
<b>Search from start</b>	<p>If selected, it searches for the specified content from the beginning of the directory. If not selected, it starts from the point in the file where it stopped reading the last time it ran.</p> <p><b>Default value:</b> Cleared</p>
<b>Run alerts</b>	<p>Select an option for alert notification:</p> <ul style="list-style-type: none"> <li>• <b>For each log entry matched.</b> The monitor triggers associated alerts according to thresholds applied to each matching entry found. Since status can change according to thresholds for each matched entry, each alert action could be triggered many times within a monitor run. For example, if 5 matches are found in each file and the total matched files is 100. then 500 alerts are triggered.</li> </ul> <p><b>Example:</b> If you want to send a warning alert on matched text value "power off" and an error alert if more than one server is turned off, set the following thresholds:</p> <ul style="list-style-type: none"> <li>• Error if matchCount &gt; 1</li> <li>• Warning if value == 'power off'</li> </ul> <p>To send an error alert if only one threshold is matched, set Error if value == 'power off'.</p> <ul style="list-style-type: none"> <li>• <b>Once, after all log entries have been checked.</b> The monitor counts up the number of matches and then triggers one alert. This is the default option.</li> </ul> <p><b>Note:</b> When <b>For each log entry matched</b> is selected: (i). Monitor performance is reduced. (ii). You should add the <code>&lt;matchedLine&gt;</code> property to the alert template to enable the monitor status to display the whole line, instead of just the matched content and the file where it was found .</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 the 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>
<b>Max File Limit</b>	<p>Limits the number of files in a given directory that can be processed. Files are processed in alphabetical order.</p> <p><b>Default value:</b> 100</p> <p><b>Note:</b> If this value exceeds the global limit set in the <code>_multiLogGlobalMaxFileLimit</code> property in the <code>&lt;SiteScope root directory&gt;\groups\master.config</code> file, then the global limit will be used instead. By default, the global limit is set to 1000.</p>

UI Element	Description
<b>Multi-line match</b>	<p>Runs a regular expression match on multiple lines of text. The monitor processes the file with a line buffer. For example, if the file contains two lines "line1" "line2", the monitor processes them as line1="line1\\n",line2=" line1\\nline2\\n"). The buffer size can be modified by changing the <b>_logFileMonitorMultiLineBufferedLines</b> value in the <b>&lt;SiteScope root directory&gt;\groups\master.config</b> file (the default value is 100).</p> <p><b>Default value:</b> Not selected</p>
<b>Server-side processing</b>	<p>Processes log file data on the remote 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>Use of this option is only recommended:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• For a log file that is frequently being written to between monitor runs. This way, all of the newly appended lines do not have to be copied across the network and parsed on the SiteScope server (the processing is done on the remote server and only the required lines would be copied across to SiteScope).</li> </ul> <p><b>Default value:</b> Not selected</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• Server-side processing is enabled for remote Linux, Red Hat Enterprise Linux, and Oracle Solaris servers only. Windows SSH is not supported.</li> <li>• To enable server-side processing to work correctly when monitoring on a Solaris server, open the remote server settings for the monitored host (<b>Remote Servers &gt; UNIX Remote Servers &gt; Main Settings</b>), and enter a path to the bash interpreter in the <b>Initialize shell environment</b> field.</li> <li>• "Rule files" are not supported in this mode.</li> <li>• The <b>/c</b> search modifier is 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>Timeout Settings</b>	
<b>Enable timeout</b>	<p>If selected, the monitor stops its run after the specified timeout period has been exceeded.</p> <p><b>Default value:</b> Selected</p>
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, that SiteScope should wait before the monitor times out.</p> <p><b>Default value:</b> 120 seconds</p> <p><b>Note:</b> This setting is only available when <b>Enable timeout</b> is selected.</p>
<b>Rules Script</b>	

UI Element	Description
<b>Enable Rules</b>	<p>If selected, the files are processed using rules. If cleared, the Rules Script box is not available (grayed out).</p> <p><b>Default value:</b> Not selected</p>
<b>&lt;Rules script&gt;</b>	<p>The rules script for processing files is displayed in this box.</p> <p>Define the rules to specify different alerts for different log entry matches. You can also set a parameter in the rules file to run script alerts. You can use any of the properties in the SiteScope Alert Template and Event Properties Directory in the Using SiteScope Guide.</p> <p>An example rules file is located in <b>&lt;SiteScope root directory&gt;\examples\log_monitor\sample.rules</b>. For instructions on how to use the file and example rules, see <a href="#">"How to Use the Rules File" on page 352</a>, or read the instructions in the file itself.</p>

## Counters

You can view details (and configure threshold settings) for the following counters:

- **fileCount** – Count of total files that matched filename regular expression.
- **filesWithMatches** – Count of files that matched search regular expression.
- **fileNames** – List of absolute file paths that match file regular expression separated by “;”. By default, the first 100 file path matches are displayed.
- **fileNamesWithMatches** – List of absolute file paths separated by “;” that matched search regular expression “;”. By default, the first 100 file path matches are displayed.
- **notProcessedFilesByTimeOut** – Files that were not processed due to timeout.
- **notProcessedFilesByLimit** – Files that were not processed by Limit.
- **values** – Matched values form regular expression. This shows only the first matched values from first file with matches.
- **matchCount** – Total matches in all files.

**Note:** You can change the number of **fileNames** and **fileNamesWithMatches** matches shown by modifying the value of the **\_multiLogFileNamesLimit** property in the **<SiteScope root directory>\groups\master.config** file. By default, the limit is set to 100. It is not recommended to increase the limit, because it significantly impacts SiteScope user interface performance.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Tips/Troubleshooting

If you encounter "Error: Can't read files." or "Error: Can't read directory." in the summary field, you should check the following:



- There was not a connection timeout.
- You have rights to read file.
- The file exists.

# Chapter 71: Network Bandwidth Monitor

This monitor enables you 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Network Bandwidth monitor.

## Learn About

This section includes:

- ["Network Bandwidth Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Performing Sanity Checks" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" on the next page](#)

## 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 a 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.

## Supported Platforms/Versions

This monitor supports monitoring remote SNMP-enabled network appliances.

## 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 sanitycheck** box in the Infrastructure Settings Preferences page (**Preferences > Infrastructure Settings Preferences > Monitor Settings**).

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences >**

**Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license for 10 monitors

# Tasks

## How to Configure the Network Bandwidth Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## Network Bandwidth Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Basic SNMP Settings</b>	
<b>Server</b>	Name of the server you want to monitor.
<b>Port</b>	Port to use when requesting data from the SNMP agent. <b>Default value:</b> 161
<b>SNMP Connection Settings</b>	
<b>Timeout (seconds)</b>	Amount of time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. <b>Default value:</b> 5 seconds
<b>Number of retries</b>	Number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. <b>Default value:</b> 1
<b>Community</b>	Community string (valid only for version 1 or 2 connections). <b>Default value:</b> public

UI Element	Description
<b>SNMP version</b>	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 fields below. <b>Default value:</b> V1
<b>Authentication algorithm</b>	Authentication algorithm to use for version 3 connections. <b>Default value:</b> MD5 <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>User name</b>	User name for version 3 connections. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Password</b>	Authentication password to use for version 3 connections. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Privacy algorithm</b>	The privacy algorithm used for authentication for SNMP version 3 (DES, 128-Bit AES, 192-Bit AES, 256-Bit AES). <b>Default value:</b> DES <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Privacy password</b>	Privacy password for version 3 connections. Leave blank if you do not want privacy. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Context engine ID</b>	Hexadecimal string representing the Context Engine ID to use for this connection. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Context name</b>	Context Name to use for this connection. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Network Counters</b>	
<b>Counters</b>	Displays 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>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on page 502</a> . <b>Note:</b> <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> </ul>

UI Element	Description
<b>Advanced Network Settings</b>	
<b>Device type</b>	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.  <b>Default value:</b> Do not monitor device-specific metrics
<b>Duplex or half-duplex</b>	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.  <b>Default value:</b> Full-duplex
<b>Interface index</b>	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.  The three possible options are: <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> <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).  <b>Default value:</b> Indexed by ifTable row number.
<b>Show bytes in/out</b>	Displays a graph for bytes in/out along with the percent bandwidth utilized on the Real-Time Metrics page.  <b>Default value:</b> Not selected
<b>Real-Time data vertical axis</b>	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>	Number of hours for which real-time graph data should be stored.  <b>Default value:</b> 24 hours

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- Bytes in
- Bytes out
- Packet in
- Packets out
- Incoming discarded packets
- Outgoing discarded packets
- Incoming packets in error
- Outgoing packets in error
- Out queue length
- % bandwidth utilization

## Tips/Troubleshooting

### General Notes/Limitations

- When working in template mode, the monitor's non-default thresholds are not copied properly to a template.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 72: News Monitor

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. This enables you to manage the number of articles that can queue up, and delete them before they cause disk space problems.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the News monitor.

## Learn About

### 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 **good**.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitored host

# Tasks

## How to Configure the News Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

**Tip:** The **News Server Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see News Server Tool in the Using SiteScope Guide.

## UI Descriptions

### News Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>News server</b>	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>	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>	User name if your News server requires authorization.
<b>Password</b>	Password if your News server requires authorization.
<b>Advanced Settings</b>	
<b>Connect from</b>	Name or IP address of the server that connects to the News monitor.
<b>Timeout (seconds)</b>	Amount of time, in 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



**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- number of articles
- round trip time
- status

# Chapter 73: Oracle 10g Application Server Monitor

Use the Oracle 10g Application Server monitor to monitor the server performance data for Oracle 10g and 10g R3 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. The error and warning thresholds for the monitor can be set on one or more Oracle 10g server performance statistics.

**Tip:** SiteScope also provides an Oracle Database 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 Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Oracle 10g Application Server monitor.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host Note: Monitor is not available when using Community edition.

## Tasks

### How to Configure the Oracle 10g Application Server Monitor

#### 1. Prerequisites

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/Apache/Apache/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 see the following URL: **http://<Oracle 10g machine URL>:7201/dmsoc4j/Spy?format=xml**.

#### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Oracle 10g Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Authorization user name</b>	User name to access the server if required.
<b>Authorization password</b>	Password to access the server if required.
<b>Proxy server</b>	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the server.
<b>Proxy server user name</b>	Proxy server user name if the proxy server requires a name and password to access the server. Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	Proxy server password if the proxy server requires a name and password to access the server. Your proxy server must support Proxy-Authenticate for these options to function.
<b>Host name</b>	Server administration URL for the server you want to monitor.
<b>Metric type</b>	The type of metrics to monitor. Options are App Server (OC4J) and Web Server (DMS).
<b>Port</b>	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 to use a secure server.
<b>Timeout (seconds)</b>	Amount of time, in 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>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> to select counters.
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a> .  <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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<p><b>Oracle HTTP Server Metrics</b></p> <ul style="list-style-type: none"> <li>• connection.active</li> <li>• connection.avg</li> <li>• connection.maxTime</li> <li>• connection.minTime</li> <li>• connection.time</li> <li>• handle.active</li> <li>• handle.avg</li> <li>• handle.maxTime</li> <li>• handle.minTime</li> <li>• handle.time</li> <li>• request.active</li> <li>• request.avg</li> <li>• request.completed</li> <li>• request.maxTime</li> <li>• request.minTime</li> <li>• request.time</li> </ul> <p><b>JVM Metrics</b></p> <ul style="list-style-type: none"> <li>• activeThreadGroups.value</li> <li>• activeThreadGroups.minValue</li> <li>• activeThreadGroups.maxValue</li> <li>• activeThreads.value</li> <li>• activeThreads.minValue</li> <li>• activeThreads.maxValue</li> <li>• upTime.value</li> <li>• freeMemory.value</li> <li>• freeMemory.minValue</li> <li>• freeMemory.maxValue</li> <li>• totalMemory.value</li> <li>• totalMemory.minValue</li> <li>• totalMemory.maxValue</li> </ul> <p><b>JDBC Metrics</b></p> <ul style="list-style-type: none"> <li>• ConnectionCloseCount.count</li> <li>• ConnectionCreate.active</li> <li>• ConnectionCreate.avg</li> <li>• ConnectionCreate.completed</li> <li>• ConnectionCreate.maxTime</li> <li>• ConnectionCreate.minTime</li> <li>• ConnectionCreate.time</li> <li>• ConnectionOpenCount.count</li> </ul> <p><b>OC4J Metrics Web Module</b></p> <ul style="list-style-type: none"> <li>• parseRequest.active</li> <li>• parseRequest.avg</li> <li>• parseRequest.completed</li> <li>• parseRequest.maxActive</li> <li>• parseRequest.maxTime</li> </ul>	<ul style="list-style-type: none"> <li>• parseRequest.minTime</li> <li>• parseRequest.time</li> <li>• processRequest.active</li> <li>• processRequest.avg</li> <li>• processRequest.completed</li> <li>• processRequest.maxActive</li> <li>• processRequest.maxTime</li> <li>• processRequest.minTime</li> <li>• processRequest.time</li> <li>• resolveContext.active</li> <li>• resolveContext.avg</li> <li>• resolveContext.completed</li> <li>• resolveContext.maxActive</li> <li>• resolveContext.maxTime</li> <li>• resolveContext.minTime</li> <li>• resolveContext.time</li> </ul> <p><b>Web Context</b></p> <ul style="list-style-type: none"> <li>• resolveServlet.time</li> <li>• resolveServlet.completed</li> <li>• resolveServlet.minTime</li> <li>• resolveServlet.maxTime</li> <li>• resolveServlet.avg</li> <li>• sessionActivation.active</li> <li>• sessionActivation.time</li> <li>• sessionActivation.completed</li> <li>• sessionActivation.minTime</li> <li>• sessionActivation.maxTime</li> <li>• sessionActivation.avg</li> <li>• service.time</li> <li>• service.completed</li> <li>• service.minTime</li> <li>• service.maxTime</li> <li>• service.avg</li> <li>• service.active</li> </ul> <p><b>Servlet</b></p> <ul style="list-style-type: none"> <li>• service.active</li> <li>• service.avg</li> <li>• service.completed</li> <li>• service.maxActive</li> <li>• service.maxTime</li> <li>• service.minTime</li> <li>• service.time</li> </ul> <p><b>JSP Runtime</b></p> <ul style="list-style-type: none"> <li>• processRequest.time</li> <li>• processRequest.completed</li> <li>• processRequest.minTime</li> </ul>	<ul style="list-style-type: none"> <li>• processRequest.maxTime</li> <li>• processRequest.avg</li> <li>• processRequest.active</li> </ul> <p><b>JSP Name</b></p> <ul style="list-style-type: none"> <li>• activeInstances.value</li> <li>• availableInstances.value</li> <li>• service.active</li> <li>• service.avg</li> <li>• service.completed</li> <li>• service.maxTime</li> <li>• service.minTime</li> <li>• service.time</li> </ul> <p><b>Session Bean</b></p> <ul style="list-style-type: none"> <li>• session-type.value</li> <li>• transaction-type.value</li> </ul> <p><b>EJB Bean</b></p> <ul style="list-style-type: none"> <li>• transaction-type.value</li> <li>• session-type.value</li> <li>• bean-type.value</li> <li>• exclusive-write-access.value</li> <li>• isolation.value</li> <li>• persistence-type.value</li> </ul> <p><b>EJB Method</b></p> <ul style="list-style-type: none"> <li>• client.active</li> <li>• client.avg</li> <li>• client.completed</li> <li>• client.maxActive</li> <li>• client.maxTime</li> <li>• client.minTime</li> <li>• client.time</li> <li>• ejbPostCreate.active</li> <li>• ejbPostCreate.avg</li> <li>• ejbPostCreate.completed</li> <li>• ejbPostCreate.maxTime</li> <li>• ejbPostCreate.minTime</li> <li>• ejbPostCreate.time</li> <li>• trans-attribute.value</li> <li>• wrapper.active</li> <li>• wrapper.avg</li> <li>• wrapper.completed</li> <li>• wrapper.maxActive</li> <li>• wrapper.maxTime</li> <li>• wrapper.minTime</li> <li>• wrapper.time</li> </ul>
---	---	--

<p><b>OPMN Info</b></p> <ul style="list-style-type: none"> <li>• default_application_log.value</li> <li>• ias_cluster.value</li> <li>• ias_instance.value</li> <li>• jms_log.value</li> <li>• oc4j_instance.value</li> <li>• oc4j_island.value</li> <li>• opmn_group.value</li> <li>• opmn_sequence.value</li> <li>• rmi_log.value</li> <li>• server_log.value</li> </ul> <p><b>JMS</b></p> <ul style="list-style-type: none"> <li>• JMSStats</li> <li>• JMSRequestHandlerStats</li> <li>• JMSConnectionStats</li> <li>• JMSSessionStats</li> <li>• JMSMessageProducerStats</li> <li>• JMSMessageBrowserStats</li> <li>• JMSMessageConsumerStats</li> <li>• JMSDurableSubscriberStats</li> <li>• JMSDestinationStats</li> <li>• JMSTemporaryDestinationStats</li> <li>• JMSStoreStats</li> <li>• JMSPersistenceStats</li> </ul> <p><b>JMS Stats Metric</b></p> <ul style="list-style-type: none"> <li>• address.value</li> <li>• connections.count</li> <li>• host.value</li> <li>• oc4j.jms.computeMsgsize.value</li> <li>• oc4j.jms.debug.value</li> <li>• oc4j.jms.doGc.value</li> <li>• oc4j.jms.expirationInterval</li> <li>• oc4j.jms.forceRecovery.value</li> <li>• oc4j.jms.intraSession.value</li> <li>• oc4j.jms.j2ee14.value</li> <li>• oc4j.jms.lazySync.value</li> <li>• oc4j.jms.listenerAttempts.</li> <li>• oc4j.jms.maxOpenFiles.value</li> <li>• oc4j.jms.messagePoll.value</li> <li>• oc4j.jms.noDms.value</li> <li>• oc4j.jms.pagingThreshold.</li> <li>• oc4j.jms.saveAllExpired.val</li> <li>• oc4j.jms.serverPoll.value</li> <li>• oc4j.jms.socketBufsize.val</li> <li>• oc4j.jms.usePersistence.val</li> <li>• oc4j.jms.useSockets.value</li> <li>• oc4j.jms.useUUID.value</li> <li>• port.value</li> <li>• requestHandlers.count</li> <li>• startTime.value</li> <li>• taskManagerInterval.value</li> <li>• method-name</li> </ul>	<p><b>JMS Request Handler Stats</b></p> <ul style="list-style-type: none"> <li>• address.value</li> <li>• connectionID.value</li> <li>• host.value</li> <li>• port.value</li> <li>• startTime.value</li> </ul> <p><b>JMS Connection Stats</b></p> <ul style="list-style-type: none"> <li>• address.value</li> <li>• clientID.value</li> <li>• domain.value</li> <li>• exceptionListener.value</li> <li>• host.value</li> <li>• isLocal.value</li> <li>• isXA.value</li> <li>• port.value</li> <li>• startTime.value</li> <li>• user.value</li> <li>• method-name</li> </ul> <p><b>JMS Session Stats</b></p> <ul style="list-style-type: none"> <li>• acknowledgeMode.value</li> <li>• domain.value</li> <li>• isXA.value</li> <li>• sessionListener.value</li> <li>• startTime.value</li> <li>• transacted.value</li> <li>• txid.value</li> <li>• xid.value</li> <li>• method-name</li> </ul> <p><b>JMS Message Producer Stats</b></p> <ul style="list-style-type: none"> <li>• deliveryMode.value</li> <li>• destination.value</li> <li>• disableMessageID.value</li> <li>• disableMessageTimestamp.value</li> <li>• domain.value</li> <li>• priority.value</li> <li>• startTime.value</li> <li>• timeToLive.value</li> <li>• method-name</li> </ul> <p><b>JMS Message Browser Stats</b></p> <ul style="list-style-type: none"> <li>• destination.value</li> <li>• selector.value</li> <li>• startTime.value</li> <li>• method-name</li> </ul>	<p><b>JMS Message Consumer Stats</b></p> <ul style="list-style-type: none"> <li>• destination.value</li> <li>• domain.value</li> <li>• messageListener.value</li> <li>• name.value</li> <li>• noLocal.value</li> <li>• selector.value</li> <li>• startTime.value</li> <li>• method-name</li> </ul> <p><b>JMS Durable Subscription Stats</b></p> <ul style="list-style-type: none"> <li>• clientID.value</li> <li>• destination.value</li> <li>• isActive.value</li> <li>• name.value</li> <li>• noLocal.value</li> <li>• selector.value</li> </ul> <p><b>JMS Destination Stats</b></p> <ul style="list-style-type: none"> <li>• domain.value</li> <li>• name.value</li> <li>• locations.value</li> <li>• method-name</li> </ul> <p><b>JMS Temporary Destination Stats</b></p> <ul style="list-style-type: none"> <li>• connectionID.value</li> <li>• domain.value</li> <li>• method-name</li> </ul> <p><b>JMS Store Stats</b></p> <ul style="list-style-type: none"> <li>• destination.value</li> <li>• messageCount.value</li> <li>• messageDequeued.count</li> <li>• messageDiscarded.count</li> <li>• messageEnqueued.count</li> <li>• messageExpired.count</li> <li>• messagePagedIn.count</li> <li>• messagePagedOut.count</li> <li>• messageRecovered.count</li> <li>• pendingMessageCount.value</li> <li>• storeSize.value</li> <li>• method-name</li> </ul> <p><b>JMS Persistence Stats</b></p> <ul style="list-style-type: none"> <li>• destination.value</li> <li>• holePageCount.value</li> <li>• isOpen.value</li> <li>• lastUsed.value</li> <li>• persistenceFile.value</li> <li>• usedPageCount.value</li> <li>• method-name</li> </ul>
---	---	---

<p><b>Taskmanager</b></p> <ul style="list-style-type: none"> <li>• interval.value</li> <li>• run().active</li> <li>• run().avg</li> <li>• run().completed</li> <li>• run().maxActive</li> <li>• run().maxTime</li> <li>• run().minTime</li> <li>• run().time</li> </ul> <p><b>mod_plsql Metrics</b></p> <p><b>Session Cache</b></p> <ul style="list-style-type: none"> <li>• cacheStatus.value</li> <li>• newMisses.count</li> <li>• staleMisses.count</li> <li>• hits.count</li> <li>• requests.count</li> </ul> <p><b>Content Cache</b></p> <ul style="list-style-type: none"> <li>• cacheStatus.value</li> <li>• newMisses.count</li> <li>• staleMisses.count</li> <li>• hits.count</li> <li>• requests.count</li> </ul> <p><b>SQLExceptionGroups</b></p> <ul style="list-style-type: none"> <li>• lastErrorDate.value</li> <li>• lastErrorRequest.value</li> <li>• lastErrorText.value</li> <li>• error.count</li> </ul> <p><b>LastNSQLErrors</b></p> <ul style="list-style-type: none"> <li>• errorDate.value</li> <li>• errorRequest.value</li> <li>• errorText.value</li> </ul> <p><b>NonSSOConnectionPool</b></p> <ul style="list-style-type: none"> <li>• connFetch.maxTime</li> <li>• connFetch.minTime</li> <li>• connFetch.avg</li> <li>• connFetch.active</li> <li>• connFetch.time</li> <li>• connFetch.completed</li> <li>• newMisses.count</li> <li>• staleMisses.count</li> <li>• hits.count</li> </ul> <p><b>RequestOwnerConnectionPool</b></p> <ul style="list-style-type: none"> <li>• connFetch.maxTime</li> <li>• connFetch.minTime</li> <li>• connFetch.avg</li> <li>• connFetch.active</li> <li>• connFetch.time</li> <li>• connFetch.completed</li> <li>• newMisses.count</li> <li>• staleMisses.count</li> <li>• hits.count</li> </ul>	<p><b>SuperUserConnectionPool</b></p> <ul style="list-style-type: none"> <li>• connFetch.maxTime</li> <li>• connFetch.minTime</li> <li>• connFetch.avg</li> <li>• connFetch.active</li> <li>• connFetch.time</li> <li>• connFetch.completed</li> <li>• newMisses.count</li> <li>• staleMisses.count</li> <li>• hits.count</li> </ul> <p><b>Portal Metrics Witness/PageEngine</b></p> <ul style="list-style-type: none"> <li>• pageRequests.value</li> <li>• cacheEnabled.value</li> <li>• cachePageHits.value</li> <li>• cachePageRequests.value</li> <li>• pageMetadataWaitTimeAvg.value</li> <li>• pageMetadataWaitTimeAvg.count</li> <li>• pageMetadataWaitTime.value</li> <li>• pageMetadataWaitTime.count</li> <li>• pageMetadataWaitTime.minValue</li> <li>• pageMetadataWaitTime.maxValue</li> <li>• pageElapsedTimeAvg.value</li> <li>• pageElapsedTimeAvg.count</li> <li>• pageElapsedTime.value</li> <li>• pageElapsedTime.count</li> <li>• pageElapsedTime.minValue</li> <li>• pageElapsedTime.maxValue</li> <li>• pageMetadataFetchTimeAvg.value</li> <li>• pageMetadataFetchTimeAvg.count</li> <li>• pageMetadataFetchTime.value</li> <li>• pageMetadataFetchTime.count</li> <li>• pageMetadataFetchTime.minValue</li> <li>• pageMetadataFetchTime.maxValue</li> <li>• queueTimeout.value</li> <li>• queueStayAvg.value</li> <li>• queueStayAvg.count</li> <li>• queueStay.value</li> <li>• queueStay.count</li> <li>• queueStay.minValue</li> <li>• queueStay.maxValue</li> </ul>	<ul style="list-style-type: none"> <li>• queueLengthAvg.value</li> <li>• queueLengthAvg.count</li> <li>• queueLength.value</li> <li>• queueLength.count</li> <li>• queueLength.minValue</li> <li>• queueLength.maxValue</li> </ul> <p><b>Witness/PageUrl</b></p> <ul style="list-style-type: none"> <li>• lastResponseDate.value</li> <li>• lastResponseCode.value</li> <li>• cacheHits.value</li> <li>• httpXXX.value</li> <li>• executeTime.maxTime</li> <li>• executeTime.minTime</li> <li>• executeTime.avg</li> <li>• executeTime.active</li> <li>• executeTime.time</li> <li>• connFetch.completed</li> </ul> <p><b>WitnessLoginUrl</b></p> <ul style="list-style-type: none"> <li>• lastResponseDate.value</li> <li>• lastResponseCode.value</li> <li>• cacheHits.value</li> <li>• httpXXX.value</li> <li>• executeTime.maxTime</li> <li>• executeTime.minTime</li> <li>• executeTime.avg</li> <li>• executeTime.active</li> <li>• executeTime.time</li> <li>• connFetch.completed</li> </ul> <p><b>WitnessVersionUrl</b></p> <ul style="list-style-type: none"> <li>• lastResponseDate.value</li> <li>• lastResponseCode.value</li> <li>• cacheHits.value</li> <li>• httpXXX.value</li> <li>• executeTime.maxTime</li> <li>• executeTime.minTime</li> <li>• executeTime.avg</li> <li>• executeTime.active</li> <li>• executeTime.time</li> <li>• connFetch.completed</li> </ul> <p><b>WitnessXSLUrl</b></p> <ul style="list-style-type: none"> <li>• lastResponseDate.value</li> <li>• lastResponseCode.value</li> <li>• cacheHits.value</li> <li>• httpXXX.value</li> <li>• executeTime.maxTime</li> <li>• executeTime.minTime</li> <li>• executeTime.avg</li> <li>• executeTime.active</li> <li>• executeTime.time</li> <li>• connFetch.completed</li> </ul>
--	---	--

<p><b>WitnessPlsqlDad-provider</b></p> <ul style="list-style-type: none"> <li>• cacheHits.value</li> <li>• offline.value</li> <li>• httpXXX.value</li> <li>• executeTime.maxTime</li> <li>• executeTime.minTime</li> <li>• executeTime.avg</li> <li>• executeTime.active</li> <li>• executeTime.time</li> <li>• connFetch.completed</li> </ul> <p><b>WitnessWebDad-provider</b></p> <ul style="list-style-type: none"> <li>• cacheHits.value</li> <li>• offline.value</li> <li>• httpXXX.value</li> <li>• executeTime.maxTime</li> <li>• executeTime.minTime</li> <li>• executeTime.avg</li> <li>• executeTime.active</li> <li>• executeTime.time</li> <li>• connFetch.completed</li> </ul> <p><b>WitnessWebDad-providerPorlet</b></p> <ul style="list-style-type: none"> <li>• lastResponseDate.value</li> <li>• lastResponseCode.value</li> <li>• cacheHits.value</li> <li>• httpXXX.value</li> <li>• executeTime.maxTime</li> <li>• executeTime.minTime</li> <li>• executeTime.avg</li> <li>• executeTime.active</li> <li>• executeTime.time</li> <li>• connFetch.completed</li> </ul> <p><b>JServ Metrics</b></p> <p><b>Overall Jserv</b></p> <ul style="list-style-type: none"> <li>• port.value</li> <li>• readRequest.active</li> <li>• readRequest.avg</li> <li>• readRequest.maxTime</li> <li>• readRequest.minTime</li> <li>• readRequest.completed</li> <li>• readRequest.time</li> <li>• maxConnections.value</li> <li>• activeConnections.maxValue</li> <li>• activeConnections.value</li> <li>• idlePeriod.maxTime</li> <li>• idlePeriod.minTime</li> <li>• idlePeriod.completed</li> <li>• idlePeriod.time</li> <li>• host.value</li> <li>• maxBacklog.value</li> </ul>	<p><b>Jserv Zone</b></p> <ul style="list-style-type: none"> <li>• checkReload.active</li> <li>• checkReload.avg</li> <li>• checkReload.maxTime</li> <li>• checkReload.minTime</li> <li>• checkReload.completed</li> <li>• checkReload.time</li> <li>• activeSessions.value</li> <li>• readSession.count</li> <li>• writeSession.count</li> <li>• loadFailed.count</li> </ul> <p><b>Jserv Servlet</b></p> <ul style="list-style-type: none"> <li>• processRequest.active</li> <li>• processRequest.avg</li> <li>• processRequest.maxTime</li> <li>• processRequest.minTime</li> <li>• processRequest.completed</li> <li>• processRequest.time</li> <li>• serviceRequest.active</li> <li>• serviceRequest.avg</li> <li>• serviceRequest.maxTime</li> <li>• serviceRequest.minTime</li> <li>• serviceRequest.completed</li> <li>• serviceRequest.time</li> <li>• loadServlet.avg</li> <li>• loadServlet.maxTime</li> <li>• loadServlet.minTime</li> <li>• loadServlet.completed</li> <li>• loadServlet.time</li> <li>• loadServletClasses.active</li> <li>• loadServletClasses.avg</li> <li>• loadServletClasses.maxTime</li> <li>• loadServletClasses.minTime</li> <li>• loadServletClasses.completed</li> <li>• loadServletClasses.time</li> <li>• loadServlet.avg</li> <li>• createSession.active</li> <li>• createSession.avg</li> <li>• createSession.maxTime</li> <li>• createSession.minTime</li> <li>• createSession.completed</li> <li>• createSession.time</li> <li>• maxSTMInstances.value</li> <li>• activeSTMInstances.maxValue</li> <li>• activeSTMInstances.value</li> </ul> <p><b>Jserv JSP</b></p> <ul style="list-style-type: none"> <li>• processRequest.active</li> <li>• processRequest.avg</li> <li>• processRequest.maxTime</li> <li>• processRequest.minTime</li> <li>• processRequest.completed</li> </ul>	<ul style="list-style-type: none"> <li>• processRequest.time</li> <li>• serviceRequest.active</li> <li>• serviceRequest.avg</li> <li>• serviceRequest.maxTime</li> <li>• serviceRequest.minTime</li> <li>• serviceRequest.completed</li> <li>• serviceRequest.time</li> <li>• loadServlet.avg</li> <li>• loadServlet.maxTime</li> <li>• loadServlet.minTime</li> <li>• loadServlet.completed</li> <li>• loadServlet.time</li> <li>• loadServletClasses.active</li> <li>• loadServletClasses.avg</li> <li>• loadServletClasses.maxTime</li> <li>• loadServletClasses.minTime</li> <li>• loadServletClasses.completed</li> <li>• loadServletClasses.time</li> <li>• loadServlet.avg</li> <li>• createSession.active</li> <li>• createSession.avg</li> <li>• createSession.maxTime</li> <li>• createSession.minTime</li> <li>• createSession.completed</li> <li>• createSession.time</li> <li>• maxSTMInstances.value</li> <li>• activeSTMInstances.maxValue</li> <li>• activeSTMInstances.value</li> </ul> <p><b>Oracle Process Manager/Notification Server Metrics</b></p> <p><b>OPMN_PM Metrics</b></p> <ul style="list-style-type: none"> <li>• jobWorkerQueue.value</li> <li>• lReq.count</li> <li>• procDeath.count</li> <li>• procDeathReplace.count</li> <li>• reqFail.count</li> <li>• reqPartialSucc.count</li> <li>• reqSucc.count</li> <li>• rReq.count</li> <li>• workerThread.value</li> </ul>
--	--	---

<p><b>OPMN_HOST_STATISTICS Metrics</b></p> <ul style="list-style-type: none"> <li>• cpuldle.value</li> <li>• freePhysicalMem.value</li> <li>• numProcessors.value</li> <li>• timestamp.value</li> <li>• totalPhysicalMem.value</li> </ul> <p><b>OPMN_IAS_INSTANCE Metrics</b></p> <ul style="list-style-type: none"> <li>• iasCluster.value</li> </ul> <p><b>OPMN_PROCESS_TYPE Metrics</b></p> <ul style="list-style-type: none"> <li>• moduleId.value</li> </ul> <p><b>OPMN_PROCESS_SET Metrics</b></p> <ul style="list-style-type: none"> <li>• numProcConf.value</li> <li>• reqFail.count</li> <li>• reqPartialSucc.count</li> <li>• reqSucc.count</li> <li>• restartOnDeath.value</li> </ul>	<p><b>OPMN_PROCESS Metrics</b></p> <ul style="list-style-type: none"> <li>• cpuTime.value</li> <li>• heapSize.value</li> <li>• iasCluster.value</li> <li>• iasInstance.value</li> <li>• indexInSet.value</li> <li>• memoryUsed.value</li> <li>• pid.value</li> <li>• privateMemory.value</li> <li>• sharedMemory.value</li> <li>• startTime.value</li> <li>• status.value</li> <li>• type.value</li> <li>• uid.value</li> <li>• upTime.value</li> </ul> <p><b>OPMN_CONNECT Metrics</b></p> <ul style="list-style-type: none"> <li>• desc.value</li> <li>• host.value</li> <li>• port.value</li> </ul>	<p><b>OPMN_ONS Metrics</b></p> <ul style="list-style-type: none"> <li>• notifProcessed.value</li> <li>• notifProcessQueue.value</li> <li>• notifReceived.value</li> <li>• notifReceiveQueue.value</li> <li>• workerThread.value</li> </ul> <p><b>OPMN_ONS_LOCAL_PORT Metrics</b></p> <ul style="list-style-type: none"> <li>• desc.value</li> <li>• host.value</li> <li>• port.value</li> </ul> <p><b>OPMN_ONS_REMOTE_PORT Metrics</b></p> <ul style="list-style-type: none"> <li>• desc.value</li> <li>• host.value</li> <li>• port.value</li> </ul> <p><b>OPMN_ONS_REQUEST_PORT Metrics</b></p> <ul style="list-style-type: none"> <li>• desc.value</li> <li>• host.value</li> <li>• port.value</li> </ul>
--	---	--

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.



# Chapter 74: Oracle 9i Application Server Monitor

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. The error and warning thresholds for the monitor can be set on one or more Oracle 9i server performance statistics.

**Tip:** SiteScope also provides an Oracle Database 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 Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Oracle 9i Application Server monitor.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric (maximum: 7)	One OSi license per monitored host

## Tasks

### How to Configure the Oracle 9i Application Server Monitor

#### 1. Prerequisites

You must enable Web caching on the Oracle 9i Application Server to use the Oracle 9i Application Server monitor.

#### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** The **URL Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see URL Tool in the Using SiteScope Guide.

## UI Descriptions

### Oracle 9i Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>URL</b>	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>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a> .
<b>Authorization user name</b>	User name if the server you want to monitor requires a name and password for access.
<b>Authorization password</b>	password if the server you want to monitor requires a name and password for access.
<b>HTTP Proxy</b>	Domain name and port of an HTTP Proxy Server. if a proxy server is used to access the server.
<b>Proxy user name</b>	Proxy server user name if the proxy server requires a name and password to access the server. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy password</b>	Proxy server password if the proxy server requires a name and password to access the server. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
<b>Timeout (seconds)</b>	Amount of time, in 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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

### Monitor Counters

Below is the list of counters that can be configured for this monitor:

**Interface: HTTP**

- Active Sessions(max)
- Active Sessions(now)
- Apology Pages Served(Network Error - number this second)
- Apology Pages Served(Network Error - total)
- Apology Pages Served(Site Busy - number this second)
- Apology Pages Served(Site Busy - total)
- Application Web Server Backlog(max)

- Application Web Server Backlog(now)
- Completed Requests(avg/sec)
- Completed Requests(max/sec)
- Completed Requests(number/sec)
- Completed Requests(total)
- Latency(avg since start)
- Latency(avg this interval)
- Load(max)
- Load(now)
- Up/Down Time(up/down)

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 75: Oracle Database Monitor

Use the Oracle Database monitor to monitor the server performance statistics from Oracle 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 Oracle Database monitor instance for each Oracle database server in your environment. The error and warning thresholds for the monitor can be set on one or more Oracle server performance statistics.

**Tip:** SiteScope also provides an Oracle Database 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 Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Oracle Database monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["Oracle Database Topology" below](#)
- ["License Consumption" on the next page](#)

### Supported Platforms/Versions

The monitor supports monitoring server performance statistics from Oracle Database 8i, 9i, 10g, 11i, 11g R2 (11.2.0.1), 11g R2 Real Application Clusters (RAC), and 12c (12.1.0.1) servers.

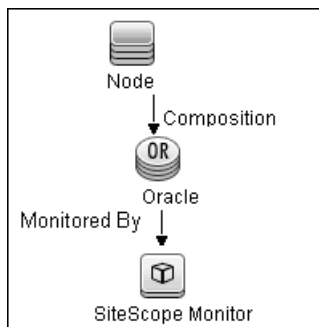
### IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the TCP (JDBC) protocol. Support for IPv6 might also depend on the JDBC driver being used.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

### Oracle Database Topology

The Oracle Database monitor can identify the topology of the Oracle databases being monitored (except for Oracle RAC databases which are not supported). The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

To ensure that the topology is reported accurately, enter the values for the **Database machine name** and the **SID**. These fields appear in the **BSM Integration Data and Topology Settings** section of **HP Integration Settings**.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host Note: Monitor is not available when using Community edition.

## Tasks

This section includes:

- ["How to Configure the Oracle Database Monitor" below](#)
- ["How to Access Oracle Databases Using OCI Driver" on page 519](#)

## How to Configure the Oracle Database Monitor

### 1. Prerequisites

The following are key requirements for using the Oracle Database monitor:

- You must have a copy of the applicable Oracle JDBC database driver file on the SiteScope server (it is recommended to use the official Oracle JDBC driver, `ojdbc6.jar` or later). Copy the downloaded driver file into the **<SiteScope root directory>\WEB-INF\lib** subdirectory. 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 `ojdbc6.jar` 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>.`

When monitoring Oracle RAC databases, the database connection URL has the form of:  
`jdbc:oracle:thin:@<server name or IP address of SCAN (Single Client Access Name) listener>:<port>/<database service name>.`

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:
  - **oracle.jdbc.driver.OracleDriver.** SiteScope supports the following categories of JDBC driver supplied by Oracle that are compatible with Java 7: JDBC thin driver for Oracle databases, and JDBC OCI (thick) driver. For details on accessing Oracle databases using OCI driver, see ["How to Access Oracle Databases Using OCI Driver" on the next page.](#)
  - **com.mercury.jdbc.oracle.OracleDriver.** A driver for Oracle databases. When using the driver deployed with SiteScope, the database connection URL has the form of:  
`jdbc:mercury:oracle://<server name or IP address>:<database server port>;sid=<sid>`

**Note:** The URL format may differ if you are using another JDBC driver, since the JDBC URL depends on the driver.

- Only one version of each driver may be installed on the SiteScope machine. If there is more than one version 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 execute SELECT queries to the following tables:
  - GV\$INSTANCE
  - GV\$STATNAME
  - GV\$SYSSTAT
  - GV\$SESSION
  - GV\$SESSTAT
  - GV\$PROCESS
  - DBA\_DATA\_FILES
  - DBA\_FREE\_SPACE
  - DBA\_DATA\_FILES
  - DBA\_DATA\_FILES

## 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## 3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in

**HP Integration Settings** (the default setting). For details on the monitor topology, see ["Oracle Database Topology" on page 516](#).

**Note:** Topology reporting for Oracle RAC databases is not supported.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

## How to Access Oracle Databases Using OCI Driver

You can monitor an Oracle database using an OCI driver. If the port or SID are changed, you only need to make the change in the **tnsnames.ora** file (the SiteScope Oracle monitors remain unchanged).

1. On the SiteScope server, install the version of Oracle client that you are using.
2. Connect to the Oracle database using the Oracle OCI driver.
  - Set **ORACLE\_HOME** environment variable (**ORACLE\_HOME** is the folder where the Oracle client or database has been installed).
  - Add **ORACLE\_HOME\lib** to System PATH (on Windows platforms), or **LD\_LIBRARY\_PATH** env variable (on UNIX platforms).
  - Set **CLASSPATH** environment variable to use Oracle JDBC driver from **ORACLE\_HOME\jdbc\lib**.
3. In the `\oracle\oraX\network\admin\tnsnames.ora` file, configure the service name. You can test this using a SQL+ tool or the SiteScope Database Connection tool (see Database Connection Tool in the Using SiteScope Guide).
4. Add a database monitor within SiteScope, and configure the following settings in the Monitor Settings panel:
  - **Database connection URL:** `jdbc:oracle:oci8:@<service name>`
  - **Database driver:** `oracle.jdbc.driver.OracleDriver`
  - Enter the database user credentials in the **Database user name** and **Database password** boxes

## UI Descriptions

### Database Connection Settings

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.

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.

User interface elements are described below:

UI Element	Description
<b>Physically close if idle connection count exceeds</b>	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. <b>Default value:</b> 10
<b>Query timeout</b>	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
<b>Idle connection timeout</b>	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>Use connection pool</b>	Enables SQL connection sharing. This means that you use a connection pool rather than open and close a new connection for each monitor query. <b>Default value:</b> Selected



## Oracle Database Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Database connection URL</b>	<p>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>When monitoring Oracle RAC databases, the database connection URL has the form of: <code>jdbc:oracle:thin:@&lt;server name or IP address of SCAN (Single Client Access Name) listener&gt;:&lt;port&gt;/&lt;service name&gt;</code>.</p> <p><b>Note:</b> The colon (:) symbol must be included as shown.</p>
<b>Database driver</b>	<p>Driver used to connect to the database.</p> <p><b>Example:</b> <code>oracle.jdbc.driver.OracleDriver</code></p>
<b>Credentials</b>	<p>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 How to Configure Credential Preferences in the Using SiteScope Guide.</li> </ul>
<b>Counters</b>	<p>Displays 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>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor (when monitoring Oracle RAC databases, these counters exist for each instance):

<p><b>GV\$SYSSTAT and GV\$SESSTAT supported using JDBC driver.</b></p> <ul style="list-style-type: none"> <li>• active txn count during cleanout</li> <li>• background checkpoints completed</li> <li>• background checkpoints started</li> <li>• background timeouts</li> <li>• branch node splits</li> <li>• buffer is not pinned count</li> <li>• buffer is pinned count</li> <li>• bytes received via SQL*Net from client</li> <li>• bytes received via SQL*Net from dblink</li> <li>• bytes sent via SQL*Net to client</li> <li>• bytes sent via SQL*Net to dblink</li> <li>• Cached Commit SCN referenced</li> <li>• calls to get snapshot scn: kcmgss</li> <li>• calls to kcmgas</li> <li>• calls to kcmgrs</li> <li>• change write time</li> <li>• cleanout - number of ktugct calls</li> <li>• cleanouts and rollbacks - consistent read gets</li> <li>• cleanouts only - consistent read gets</li> <li>• cluster key scan block gets</li> <li>• cluster key scans</li> <li>• cold recycle reads</li> <li>• commit cleanout failures: block lost</li> <li>• commit cleanout failures: buffer being written</li> <li>• commit cleanout failures: callback failure</li> <li>• commit cleanout failures: cannot pin</li> <li>• commit cleanout failures: hot backup in progress</li> <li>• commit cleanout failures: write disabled</li> </ul>	<ul style="list-style-type: none"> <li>• commit cleanouts</li> <li>• commit cleanouts successfully completed</li> <li>• Commit SCN cached</li> <li>• commit txn count during cleanout</li> <li>• consistent changes</li> <li>• consistent gets</li> <li>• consistent gets - examination</li> <li>• CPU used by this session</li> <li>• CPU used when call started</li> <li>• CR blocks created</li> <li>• current blocks converted for CR</li> <li>• cursor authentications</li> <li>• data blocks consistent reads - undo records applied</li> <li>• db block changes</li> <li>• db block gets</li> <li>• DBWR buffers scanned</li> <li>• DBWR checkpoint buffers written</li> <li>• DBWR checkpoints</li> <li>• DBWR cross instance writes</li> <li>• DBWR free buffers found</li> <li>• DBWR fusion writes</li> <li>• DBWR lru scans</li> <li>• DBWR make free requests</li> <li>• DBWR revisited being-written buffer</li> <li>• DBWR summed scan depth</li> <li>• DBWR transaction table writes</li> <li>• DBWR undo block writes</li> <li>• DDL statements parallelized</li> <li>• deferred (CURRENT) block cleanout applications</li> <li>• deferred CUR cleanouts (index blocks)</li> <li>• DFO trees parallelized</li> <li>• dirty buffers inspected</li> <li>• DML statements parallelized</li> <li>• enqueue conversions</li> <li>• enqueue deadlocks</li> <li>• enqueue releases</li> <li>• enqueue requests</li> <li>• enqueue timeouts</li> </ul>	<ul style="list-style-type: none"> <li>• enqueue waits</li> <li>• exchange deadlocks</li> <li>• execute count</li> <li>• free buffer inspected</li> <li>• free buffer requested</li> <li>• gcs messages sent</li> <li>• ges messages sent</li> <li>• global cache blocks corrupt</li> <li>• global cache blocks lost</li> <li>• global cache claim blocks lost</li> <li>• global cache convert time</li> <li>• global cache convert timeouts</li> <li>• global cache converts • global cache cr block build time</li> <li>• global cache cr block flush time</li> <li>• global cache cr block receive time</li> <li>• global cache cr block send time</li> <li>• global cache cr blocks received</li> <li>• global cache cr blocks served</li> <li>• global cache current block flush time</li> <li>• global cache current block pin time</li> <li>• global cache current block receive time</li> <li>• global cache current block send time</li> <li>• global cache current blocks received</li> <li>• global cache current blocks served</li> <li>• global cache defers</li> <li>• global cache freelist waits</li> <li>• global cache get time</li> <li>• global cache gets</li> <li>• global cache prepare failures</li> <li>• global cache skip prepare failures</li> </ul>
--	---	--

<ul style="list-style-type: none"> <li>• global lock async converts</li> <li>• global lock async gets</li> <li>• global lock convert time</li> <li>• global lock get time</li> <li>• global lock releases</li> <li>• global lock sync converts</li> <li>• global lock sync gets</li> <li>• hot buffers moved to head of LRU</li> <li>• immediate (CR) block cleanout applications</li> <li>• immediate (CURRENT) block cleanout applications</li> <li>• immediate CR cleanouts (index blocks)</li> <li>• index fast full scans (direct read)</li> <li>• index fast full scans (full)</li> <li>• index fast full scans (rowid ranges)</li> <li>• index fetch by key</li> <li>• index scans kdiixs1</li> <li>• instance recovery database freeze count</li> <li>• kcmccs called get current scn</li> <li>• kcmgss read scn without going to GES</li> <li>• kcmgss waited for batching</li> <li>• leaf node 90-10 splits</li> <li>• leaf node splits</li> <li>• logons cumulative</li> <li>• logons current</li> <li>• messages received</li> <li>• messages sent</li> <li>• native hash arithmetic execute</li> <li>• native hash arithmetic fail</li> <li>• next scns gotten without going to GES</li> <li>• no buffer to keep pinned count</li> <li>• no work - consistent read gets</li> <li>• number of map misses</li> <li>• number of map operations</li> <li>• opened cursors cumulative</li> <li>• opened cursors current</li> <li>• opens of replaced files</li> <li>• opens requiring cache replacement</li> <li>• OS All other sleep time</li> <li>• OS Chars read and written</li> <li>• OS Data page fault sleep time</li> <li>• OS Input blocks</li> <li>• OS Involuntary context switches</li> <li>• OS Kernel page fault sleep time</li> <li>• OS Major page faults</li> <li>• OS Messages received</li> <li>• OS Messages sent</li> <li>• OS Minor page faults</li> <li>• OS Other system trap CPU time</li> <li>• OS Output blocks</li> <li>• OS Process heap size</li> <li>• OS Process stack size</li> </ul>	<ul style="list-style-type: none"> <li>• OS Swaps</li> <li>• OS System call CPU time</li> <li>• OS System calls</li> <li>• OS Text page fault sleep time</li> <li>• OS User level CPU time</li> <li>• OS User lock wait sleep time</li> <li>• OS Voluntary context switches •</li> <li>• OS Wait-cpu (latency) time</li> <li>• OTC commit optimization attempts</li> <li>• OTC commit optimization failure - setup</li> <li>• OTC commit optimization hits</li> <li>• Parallel operations downgraded 1 to 25 pct</li> <li>• Parallel operations downgraded 25 to 50 pct</li> <li>• Parallel operations downgraded 50 to 75 pct</li> <li>• Parallel operations downgraded 75 to 99 pct</li> <li>• Parallel operations downgraded to serial</li> <li>• Parallel operations not downgraded</li> <li>• parse count (failures)</li> <li>• parse count (hard)</li> <li>• parse count (total)</li> <li>• parse time cpu</li> <li>• parse time elapsed</li> <li>• physical reads</li> <li>• physical reads direct</li> <li>• physical reads direct (lob)</li> <li>• physical writes</li> <li>• physical writes direct</li> <li>• physical writes direct (lob)</li> <li>• physical writes non checkpoint</li> <li>• pinned buffers inspected</li> <li>• prefetch clients - 16k</li> <li>• prefetch clients - 2k</li> <li>• prefetch clients - 32k</li> <li>• prefetch clients - 4k</li> <li>• prefetch clients - 8k</li> <li>• prefetch clients - default</li> <li>• prefetch clients - keep</li> <li>• prefetch clients - recycle</li> <li>• prefetched blocks</li> <li>• prefetched blocks aged out before use</li> <li>• process last non-idle time</li> <li>• PX local messages rcv'd</li> <li>• PX local messages sent</li> <li>• PX remote messages rcv'd</li> <li>• PX remote messages sent</li> <li>• queries parallelized</li> <li>• recovery array read time</li> <li>• recovery array reads</li> </ul>	<ul style="list-style-type: none"> <li>• redo blocks written</li> <li>• redo buffer allocation retries</li> <li>• redo entries</li> <li>• redo log space requests</li> <li>• redo log space wait time</li> <li>• redo log switch interrupts</li> <li>• redo ordering marks• redo size</li> <li>• redo synch time</li> <li>• redo synch writes</li> <li>• redo wastage</li> <li>• redo write time</li> <li>• redo writer latching time</li> <li>• redo writes</li> <li>• remote instance undo block writes</li> <li>• remote instance undo header writes</li> <li>• rollback changes - undo records applied</li> <li>• rollbacks only - consistent read gets</li> <li>• RowCR - row contention</li> <li>• RowCR attempts</li> <li>• RowCR hits</li> <li>• rows fetched via callback</li> <li>• serializable aborts</li> <li>• session connect time</li> <li>• session cursor cache count</li> <li>• session cursor cache hits</li> <li>• session logical reads</li> <li>• session pga memory</li> <li>• session pga memory max</li> <li>• session stored procedure space</li> <li>• session uga memory</li> <li>• session uga memory max</li> <li>• shared hash latch upgrades - no wait</li> <li>• shared hash latch upgrades - wait</li> <li>• sorts (disk)</li> <li>• sorts (memory)</li> <li>• sorts (rows)</li> <li>• SQL*Net roundtrips to/from client</li> <li>• SQL*Net roundtrips to/from dblink</li> <li>• summed dirty queue length</li> <li>• switch current to new buffer</li> <li>• table fetch by rowid</li> <li>• table fetch continued row</li> <li>• table lookup prefetch client count</li> <li>• table scan blocks gotten</li> <li>• table scan rows gotten</li> <li>• table scans (cache partitions)</li> </ul>
--	--	---

<ul style="list-style-type: none"> <li>• OS Signals received</li> </ul>	<ul style="list-style-type: none"> <li>• recovery blocks read</li> <li>• recursive calls</li> <li>• recursive cpu usage</li> </ul>	
<ul style="list-style-type: none"> <li>• transaction lock background get time</li> <li>• transaction lock background gets</li> <li>• transaction lock foreground requests</li> <li>• transaction lock foreground wait time</li> <li>• transaction rollbacks</li> <li>• transaction tables consistent read rollbacks</li> </ul>	<ul style="list-style-type: none"> <li>• transaction tables consistent reads - undo records applied</li> <li>• Unnecessary process cleanup for SCN batching</li> <li>• user calls</li> <li>• user commits</li> <li>• user rollbacks</li> <li>• workarea executions - multipass</li> <li>• workarea executions - onepass</li> <li>• workarea executions - optimal</li> </ul>	<ul style="list-style-type: none"> <li>• workarea memory allocated</li> <li>• write clones created in background</li> <li>• write clones created in foreground</li> <li>• table scans (direct read)</li> <li>• table scans (long tables)</li> <li>• table scans (rowid ranges)</li> <li>• table scans (short tables)</li> <li>• total file opens</li> <li>• total number of slots</li> </ul>

## Tips/Troubleshooting

### General Notes/Limitations

- 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.
- For information about troubleshooting the Oracle Database monitor, see [HPE Software Self-solve Knowledge Base](https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM189298) (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM189298). To enter the knowledge base, you must log on with your HPE Passport ID.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- Topology reporting for Oracle RAC databases is not supported.
- By default, the set of monitor counters for each session has been limited to avoid a Java Heap Space error on the applet side where the Oracle Database has a large number of sessions. You can manage the set of session counters in the **Oracle Database session counters** setting in **Preferences > Infrastructure Preferences > Monitor Settings**. For details, see Monitor Settings in the Infrastructure Preferences section of the Using SiteScope Guide.

# Chapter 76: Ping Monitor

The Ping monitor enables you to check the availability of a host by using ICMP (Internet Control Message Protocol). Use this monitor to check network connectivity and response time.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Ping monitor.

## Learn About

This section includes:

- ["Ping Monitor Overview" below](#)
- ["What to Monitor" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" on the next page](#)

## 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.

## 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.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the ICMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license for 10 monitors

## Tasks

### How to Configure the Ping Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** The **Ping Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Ping Tool in the Using SiteScope Guide.

## UI Descriptions

### Ping Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Host name to resolve</b>	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>Note:</b> You can monitor only one IP or host name at a time for each monitor instance.
<b>Packet size (bytes)</b>	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. <b>Default value:</b> 32 bytes
<b>Timeout (milliseconds)</b>	Amount of time, in milliseconds, that should pass before the ping times out. To change the threshold, enter the new value in the text box. <b>Default value:</b> 5000 milliseconds

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Tips/Troubleshooting

## General Notes/Tips

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.
- The **round trip time** counter is both measured and displayed in the SiteScope Dashboard in milliseconds; for all other monitors, it is measured in milliseconds and displayed in seconds.

# Chapter 77: Port Monitor

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 after the connection is made. You can 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Port monitor.

## Learn About

This section includes:

- ["Status" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" on the next page](#)

## 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.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the TCP and UDP protocols.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.



## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license for 10 monitors

## Tasks

### How to Configure the Port Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** The **Ping Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Ping Tool in the Using SiteScope Guide.

## UI Descriptions

### Port Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Host name</b>	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>	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 <b>&lt;SiteScope root directory&gt;\groups\master.config</b> file.
<b>Timeout (seconds)</b>	Amount of time, in seconds, to 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>	Customizes the string sent to the host after a connection is made.

UI Element	Description
<b>Match string</b>	<p>Checks 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.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"><li>• The search is case sensitive.</li><li>• You cannot use regular expressions in this field.</li></ul>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- port response
- round trip time
- status

Supports both TCP and UDP (UDP requires additional configuration)

## Tips/Troubleshooting

### Tips

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.

# Chapter 78: Radius Monitor

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. A RADIUS server is used to authenticate users, often connecting through a remote connection such as a dialup modem or a DSL line. If the RADIUS server fails, any users that try to use it are unable to log on and access any services.

Create a separate monitor instance for each server you are running. You may want to set up multiple monitors per server if you want to test different kinds of login accounts.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Radius monitor.

## Learn About

### 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**.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	1 OSi license per monitored host

## Tasks

### How to Configure the Radius Monitor

1. Prerequisites
  - 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 can communicate with. This must be done 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.
2. Configure the monitor properties  
Configure the monitor properties as required.  
For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Radius Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Radius server</b>	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>	Secret used to encrypt all requests to this RADIUS server.
<b>User name</b>	User name to authenticate.
<b>Password</b>	Password to authenticate.
<b>Called Station Id</b>	Telephone number on which the call was received. For virtual private network (VPN) connections, the IP address of the VPN server.
<b>Calling Station Id</b>	Telephone number from which the call was made. For virtual private network (VPN) connections, the IP address of the VPN client.
<b>Port</b>	UDP port used by the RADIUS server. <b>Default value:</b> 1812
<b>Timeout (seconds)</b>	Amount of time, in seconds, to wait for the connection to the port, and for any sending and receiving to complete. Once this time period passes, the Radius monitor logs an error and reports an error status. <b>Default value:</b> 30 seconds

UI Element	Description
<b>Match content</b>	<p>Text string to check for in the response. If the text is not contained in the response, the monitor displays the message no match on content.</p> <p>You can 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> / \d\d/ or /size \d\d/i</p> <p><b>Note:</b> The search is case sensitive.</p>
<b>Open Tool</b>	<p>Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

Authentication request

- match value
- round trip time
- status

# Chapter 79: Real Media Player Monitor (Deprecated)

**Note:** The Real Media Player monitor was deprecated, and is currently not planned for future versions of SiteScope. If this monitor was configured in a previous version of SiteScope, it is still displayed in SiteScope after performing an upgrade (but will not work). This monitor is supported in SiteScope 11.24 and earlier versions.

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.

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. The error and warning thresholds for the monitor can be set on one or more Real Media Player performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Real Media Player monitor.

## Learn About

### Supported Platforms/Versions

- This monitor is supported in SiteScopes that are running on Windows versions only.
- This monitor supports monitoring RealNetworks Real Media Player versions 7.x, 8.x, 9.x, and 10.x
- This monitor does not support metadata files such as the .smi format.

## Tasks

### How to Configure the Real Media Player Monitor

#### 1. Prerequisites

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.

#### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Real Media Player Monitor Settings

User interface elements are described below:

UI Element	Description
<b>URL</b>	<p>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>Counters</b>	<p>Select the server performance counters you want to check with this monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</p>
<b>Duration (milliseconds)</b>	<p>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> 15,000 milliseconds</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

### Monitor Counters

Below is the list of counters that can be configured for this monitor:

- bandwidth
- buffering congestion num
- buffering congestion time
- buffering num
- buffering seek num
- buffering seek time
- buffering time
- first frame time
- late packets
- live pause num
- live pause time
- lost packets
- network performance
- recovered packets
- stream quality

# Chapter 80: Real Media Server Monitor

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Real Media Server monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" on the next page](#)

## Supported Platforms/Versions

This monitor is supported in SiteScopes running on Windows platforms, and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.



## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host

# Tasks

## How to Configure the Real Media Server Monitor

### 1. Prerequisites

- Make sure you have the specific access permissions required for this monitor as specified in Permissions and Credentials.
- The Real Media Server monitor makes use of Performance Counters to measure application server performance. SiteScopes running on Windows platforms need 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. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Note:** 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**.

## UI Descriptions

### Real Media Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of the server 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></p> <ul style="list-style-type: none"><li>• 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 <i>Configure the WMI Service for Remote Monitoring</i> in the <i>Using SiteScope Guide</i>.</li><li>• When working in template mode, 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></ul> <p><b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)</p>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 <i>How to Configure SiteScope to Monitor a Remote Microsoft Windows Server</i> in the <i>Using SiteScope Guide</i>.</p>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see <i>New/Edit Microsoft Windows Remote Server Dialog Box</i> in the <i>Using SiteScope Guide</i>.</p>

UI Element	Description
<b>Counters</b>	<p>Displays 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>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see "<a href="#">Monitor Counters</a>" below.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- Encoder Connections
- HTTP Clients
- Monitor Connections
- Multicast Connections
- PNA Clients
- RTSP Clients
- Splitter Connections
- TCP Connections
- Total Bandwidth
- Total Clients
- UDP Clients

## Tips/Troubleshooting

### General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 81: REST API Monitor

SiteScope REST API monitor enables monitoring the performance of software that provide their counters in the form of JSON or XML through HTTP/HTTPS interfaces using REST API calls. Some examples of software that can be monitored using the REST API monitor are Mongo DB, GlassFish AS, and Docker. Using this monitor you can also monitor your REST Web Services.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the REST API monitor.

## Learn About

### Supported Platforms/Versions

This monitor supports monitoring all software that provide their counters in the form of JSON or XML representation through REST API HTTP/HTTPS methods.

### 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 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 ["REST API Monitor Settings" on page 542](#).
- Importing the server certificate. For details on how to perform this task, see ["How to Configure the REST API Monitor" on the next page](#).

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol/HTTP Client used by SiteScope	Support
SSLv3	√
TLSv1.0, TLSv1.1, TLSv1.2	√

### License Consumption

Point-based Usage	Capacity-based Usage
One point per monitored URL	One URL license per monitored URL

# Tasks

## How to Configure the REST API Monitor

### 1. Prerequisites

- The user name and password specified in the Credentials field (in Authentication Settings) must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.
- **JSON Response Requirements** - Responses in JSON format must support ECMA-404 standard for JavaScript Object Notation and have application/json internet media type.
- **XML Response Requirements** - SiteScope parses the XML content based on the following assumptions:
  - The XML content has only one root node. This means that all 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 in the following format:  

```
<node_tag>node_value</node_tag>
```

where `<node_tag>` is the counter name and `<node_value>` is the counter value.
  - Each leaf node (and therefore each counter) has a unique path within the hierarchy of the XML content.
  - The XML metric file contains at least one leaf node.

If your XML metric file does not conform to these rules, you can specify an eXtensible Stylesheet Language: Transformations (XSLT) file that transforms your XML file into a file that conforms. Such a file usually has a file extension of .xsl.

SiteScope provides the XSL Transformation tool that enables you to verify the transformation output. For more information, see XSL Transformation Tool.

### 2. 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 How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
- Import the server certificates manually. For details, see ["How to Manually Import Server Certificates" below](#).

### 3. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## How to Manually Import Server Certificates

Instead of using Certificate Management, you can manually import certificates 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 in the Using SiteScope Guide.

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.

## UI Descriptions

### REST API Monitor Settings

User interface elements are described below:

UI Element	Description
<b>HTTP Request Settings</b>	
URL	<p>URL of the monitored software.</p> <p>Example (in bold): <b>http://www.company.com:4848/hostInfo/json=1</b></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>Example (in bold): <b>https://www.company.com:4848/hostInfo/json=1</b></p> <p>For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on page 545</a>.</p>
Port	<p>Port number used by the software for providing access through HTTP or HTTPS.</p> <p>Example (in bold): http://www.company.com:<b>4848</b>/hostInfo/json=1</p>
Resource	<p>Resource of the monitored software.</p> <p>Example (in bold): http://www.company.com:4848/<b>hostInfo/json=1</b></p>

UI Element	Description
HTTP Method	<p>HTTP method that will be used for the request.</p> <ul style="list-style-type: none"> <li>• GET — Send GET request.</li> <li>• POST — Send POST request.</li> <li>• PUT — Send PUT request.</li> <li>• DELETE — Send DELETE request.</li> </ul> <p>Default value: GET</p> <p>Example (in bold): <code>http://www.company.com:4848/hostInfo/<b>json=1</b></code></p>
Query Parameters	<p>Query parameters to be passed through the HTTP request. Query parameters should be added one per line as name=value pairs.</p>
Request Headers	<p>Header request lines sent by the HTTP client to the server. Headers must be separated by a line break.</p> <p>The standard list of HTTP/1.1 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>
<b>HTTP Response Settings</b>	
Response Type	<p>Type of response that SiteScope expects to receive from the monitored software.</p> <ul style="list-style-type: none"> <li>• JSON — Javascript Object Notation is a data format commonly used for response body.</li> <li>• XML — Extensible markup language is a format that is used to describe documents and data.</li> </ul> <p>Default value: JSON</p>
XSL file	<p>Convert the XML metrics file into a format that SiteScope can use. Enable for XML response type only.</p>
<b>Proxy settings</b>	
HTTP proxy	<p>Domain name and port of an HTTP proxy server if a proxy server is used to access the URL.</p>
Proxy server user name	<p>Proxy server user name if the proxy server requires a user name to access the URL.</p> <p>Note: Your proxy server must support Proxy-Authenticate for this option to function.</p>
Proxy server password	<p>Proxy server password if the proxy server requires a user name to access the URL.</p> <p>Note: Your proxy server must support Proxy-Authenticate for this option to function.</p>
Proxy NTLM V2	<p>Select this option if the proxy server requires authentication using NTLM version 2.</p>
<b>Authentication Settings</b>	

UI Element	Description
Credentials	<p>Option to use for authorizing credentials if the URL specified requires a name and password for access:</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 Credential profile drop-down list, or click <b>Add Credentials</b> and create a new credential profile. For details on how to perform this task, see How to Configure Credential Preferences.</li> </ul>
Pre-emptive authorization	<p>Option for sending authorization credentials if SiteScope requests the target URL:</p> <ul style="list-style-type: none"> <li>• <b>Use global preference.</b> Select this option to have SiteScope use the setting specified in the Pre-emptive authorization section of the General Preferences page.</li> <li>• <b>Authenticate first request.</b> Select this option to send the user name and password on the first request SiteScope makes for the target URL.</li> </ul> <p>Note: If the URL does not require a user name and password, this option may cause the URL to fail.</p> <ul style="list-style-type: none"> <li>• <b>Authenticate if requested.</b> Select this option to send the user name and password on the second request if the server requests a user name and password.</li> </ul> <p>Note: If the URL does not require a user name and password, this option may be used. All options use the User name and Password entered for this monitor instance. If these are not specified for the individual monitor, the Default authentication user name and Default authentication password specified in the Main section of the General Preferences page are used, if they have been specified.</p> <p>Note: 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>
Client side certificate	<p>The certificate file, if you need to use a client side certificate to access the target URL. This is a .pfx (.p12) type certificate, which usually requires a password. Enter the password for the certificate in the Client side certificate password box.</p> <p>Note: Client side certificate files must be copied into the &lt;SiteScope root directory&gt;\templates.certificates directory.</p>
Client side certificate password	<p>Password if you are using a client side certificate and that certificate requires a password.</p>
Authorization NTLM domain	<p>Domain for NT LAN Manager (NTLM) authorization if required to access the URL.</p>



UI Element	Description
Accept untrusted certificates for HTTPS	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 <a href="#">SSL Connectivity</a> .
Accept invalid certificates for HTTPS	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.
NTLM V2	Select this option if the URL you are accessing requires authentication using NTLM version 2.
Preferred protocols	<p>Select the preferred protocol option to use for the handshake process.</p> <ul style="list-style-type: none"> <li>• <b>Any supported protocol.</b> Enables any supported protocol to be used for the handshake process (this is the default setting). Since this option uses SSL protocols, SSL must be enabled on the Web server to use this option.</li> <li>• <b>Prefer SSL to TLS.</b> Select this option if the URL you are accessing cannot handle authentication using TLS. This enables encrypted handshake messages to be sent using SSL. Note: This option is ignored (if selected) when SiteScope is running in FIPS 140-2 mode, since authentication using TLS is mandatory with FIPS 140-2. For details on FIPS 140-2, see the Running SiteScope Securely section of the SiteScope Deployment Guide (available from the SiteScope 11.32 Planning and Deployment Documentation page).</li> <li>• <b>Prefer TLS to SSL.</b> Select this option if you prefer to use TLS for encrypting handshake messages or if the URL you are accessing cannot handle authentication using SSL. TLS is the latest cryptographic protocol. TLS 1.0, 1.1, and 1.2 are supported.</li> </ul>
<b>Counters</b>	
Counters	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
Get Counters	Opens the <b>Select Counters</b> Form, enabling you to select the counters you want to monitor. This tree of counters is based on response from the monitored software.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

REST API monitor provides the following set of default counters which are available for all monitored software. This is in addition to the counters from the monitored software.

- response – Response from the monitored software.
- response status code – Response HTTP status code from the monitored software.

- response status line – Response status line from the monitored software.
- response status text – Response status text from the monitored software.
- response charset – Charset of response from the monitored software.
- response headers – Headers of response from the monitored software.
- request duration (milliseconds) – Duration of HTTP/HTTPS request to the monitored software.

## Tips/Troubleshooting

This section describes troubleshooting and limitations for the REST API monitor.

### General Notes/Tips

- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- You might encounter error in fetching counters if you have not specified the port. If you encounter such an error, provide the port number to fetch counters from the monitor.

### Troubleshooting Logs

The `rest_monitor.log` file (located in `<SiteScope root directory>\logs\`) provides information about REST API monitor errors and debug information.

To view REST API monitor errors and debug information, copy the following sections from the `log4j.properties.debug` file in the `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava` folder to the `log4j.properties` file, and change the log level to `DEBUG`.

```
#####  
# REST API monitor  
#####  
log4j.category.com.mercury.sitescope.monitors.facades.RestApiMonitor=DEBUG,  
rest.monitor.appender  
  
log4j.additivity.com.mercury.sitescope.monitors.facades.RestApiMonitor=false  
log4j.category.com.mercury.sitescope.monitors.http.rest=DEBUG, rest.monitor.appender  
log4j.additivity.com.mercury.sitescope.monitors.http.rest=false  
log4j.appender.rest.monitor.appender=org.apache.log4j.RollingFileAppender  
log4j.appender.rest.monitor.appender.File=../${log.file.path}/rest_monitor.log  
log4j.appender.rest.monitor.appender.MaxFileSize=${def.file.max.size}  
log4j.appender.rest.monitor.appender.MaxBackupIndex=${def.files.backup.count}  
log4j.appender.rest.monitor.appender.layout=org.apache.log4j.PatternLayout  
log4j.appender.rest.monitor.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n  
log4j.appender.rest.monitor.appender.encoding=${general.encoding}
```

# Chapter 82: SAP CCMS Monitor

The SAP CCMS monitor enables you to monitor the performance of your SAP R/3 System landscape in a centralized manner using SAP's centralized monitoring architecture, CCMS (Computer Center Management System).

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of SAP monitoring. For details, see SAP Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP CCMS monitor.

## Learn About

This section includes:

- ["SAP CCMS Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["SAP CCMS Topology" below](#)
- ["License Consumption" on the next page](#)

### SAP CCMS Monitor Overview

Use the SAP CCMS monitor to retrieve and report metrics using SAP's centralized monitoring architecture, CCMS. With CCMS, a SAP administrator can monitor all servers, components and resources in the SAP landscape from a single centralized server, greatly facilitating not only problem discovery but also problem diagnosis.

Using the SAP CCMS monitor, you can also enable reporting of the host topology to BSM. If enabled, BSM automatically populates the RTSM with CIs based on the monitored hardware in SiteScope.

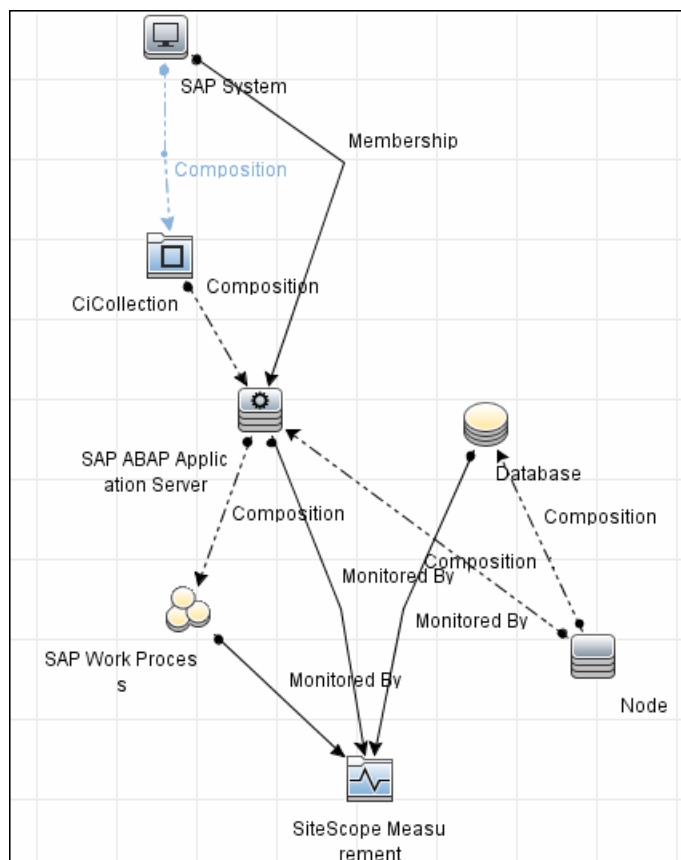
Using SAP's advanced CCMS interface BC-XAL 1.0, the SiteScope SAP CCMS monitor exposes hundreds of performance and availability metrics. The error and warning thresholds for the monitor can be set for one or more of the nearly 120 SAP server performance statistics available by using the CCMS interface.

### Supported Platforms/Versions

This monitor supports monitoring 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.

### SAP CCMS Topology

The SAP CCMS monitor can identify the topology of the SAP System being monitored. The monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM as SiteScope Measurement Groups and SiteScope Measurement CIs.

**Note:**

- This direct integration between SiteScope and BSM is available only when the Application Management for SAP license is installed.
- When you add a new application server to the SAP System, you must clear the **Report monitor and related CI topology** 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 details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

For information about the SAP topology, see SAP Systems View in the BSM User Guide in the BSM Help.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host Note: Monitor is not available when using Community Edition.

# Tasks

## How to Configure the SAP CCMS Monitor

### 1. Prerequisites

- Before configuring the monitor, make sure you have the necessary setup requirements and user privileges to log on to the CCMS server and retrieve metrics.
  - The SAP Java Connector (SAP JCo 3.x) component must be installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location). For details, see step 3 below.
  - You must have SAP authorization of the remote system user. For details on the SAP permissions required by SiteScope, see ["SAP Permissions" below](#)
  - Consult your SAP documentation to determine if your R/3 landscape components requires additional software installed to run or work with CCMS.

**Note:** The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and later only.

- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries.

### 2. SAP Permissions

- The following is the minimal set of SAP authorizations required by SiteScope in order to create and retrieve the necessary data from the monitor:

RFC1, SALX, SDIF\*, SXMI, SYST, SYSU

S_RFC – Authorization check for RFC access	
Activity	16 (Execute)
Name of RFC to be protected	SXMI, SALX, SYST
Type of RFC object to be protected	FUGR

- Alternatively, you can set certain privileges for SAP user 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 log on 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 user interface and see if the CCMS monitor sets can be displayed.

### 3. Download the SAP Java Connector

The SAP 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.

Download and install the SAP Java Connector 3.x component to the server where SiteScope is running (or at least it must be accessible on a shared or remote location).

- a. Log on 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. After you log on, select **SAP NetWeaver > SAP NetWeaver in Detail > Application Platform > Connectivity > Connectors > SAP Java Connector**, and then click **Tools and Services**.
- c. Before downloading JCo 3.x.jar and .dll files, you must perform the following:
  - Remove any previously installed **sapjco.jar** files before downloading the JCo 3.x files.
  - Set the **SAP Java Connector version** property in **Preferences > Infrastructure Preferences > Monitor Settings** to **3.x**.
- d. Download the JCo 3.x.jar and .dll files from the SAP support Web site:

On a Windows environment, download:

File	Copy to...
sapjco3.jar	<SiteScope root directory>\WEB-INF\lib
sapjco3.dll	<SiteScope root directory>\bin

On a UNIX environment, download:

File	Copy to...
sapjco3.jar	<b>&lt;SiteScope root directory&gt;/WEB-INF/lib</b> <b>Note:</b> JCO native libraries must be copied to <b>/usr/lib64</b> . To check that a JCO connector is installed correctly, run the following command: <code>/opt/HP/SiteScope/java/bin/java -jar /opt/HP/SiteScope/WEB-INF/lib/sapjco3.jar</code>
libsapjco3.so	<ul style="list-style-type: none"> <li>◦ For Sun installations: <b>&lt;SiteScope root directory&gt;/java/lib/sparc</b></li> <li>◦ For Linux installations: <b>/usr/lib64</b></li> </ul>

- e. Restart SiteScope.

#### 4. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

#### 5. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "[SAP CCMS Topology](#)" on page 547.

For user interface details, see BSM Integration Data and Topology Settings in the Using SiteScope Guide.

## UI Descriptions

### SAP CCMS Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Application server</b>	Address of the SAP server you want to monitor.
<b>SAP client</b>	Client to use for connecting to SAP.
<b>System number</b>	System number for the SAP server.
<b>SAP router string</b>	<p>Router address string if your connection is being made through a router (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>Option for providing the user name and password 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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>CCMS monitor sets match</b>	Enter a regular expression to match the SAP CCMS monitor sets you want to view (top level nodes of the CCMS tree). Only counters of matched tree sets are requested from SAP and displayed in the counter tree. To change the match, you must reload the counters. If the field is empty, all monitor sets are shown.
<b>Collect all types of counters</b>	<p>Select to enable the monitor to collect all other types of counters in addition to collecting SAP performance counters.</p> <p><b>Note:</b> If this option is selected, it is recommended to use <b>CCMS monitor sets match</b> to prevent performance capacity problems.</p>
<b>Counters</b>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.

UI Element	Description
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. This tree displays the hierarchy of Monitoring Tree Elements that is shown in the SAP user interface with transaction RZ20. The information in the SiteScope browse tree may differ slightly from that in RZ20 depending on the authorization level of the user name you specified for this monitor. For details, see <a href="http://help.sap.com/saphelp_erp60_sp/helpdata/en/f0/4f70403590ca01e10000000a155106/frameset.htm">http://help.sap.com/saphelp_erp60_sp/helpdata/en/f0/4f70403590ca01e10000000a155106/frameset.htm</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Tips

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

### 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.
- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries
- By default, the SAP client library (librfc32u.dll) supports a maximum of 100 connections to the SAP system. If you exceed this number of connections, an exception will be thrown (ERROR max no of 100 conversations exceeded). For this reason, you should set the CPIC\_MAX\_CONV environment variable to increase the number of connections supported by the SAP client library. If you change CPIC\_MAX\_CONV, you must restart your computer for the change to take effect.
- 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.
- After a SAP system restart, the value of specific IDs (mtUID) can change, resulting in the SAP CCMS monitor returning n/a for some counters. If this occurs, it continues until you reload the monitored counter in the monitor properties.  
**Workaround:** To avoid losing the SAP system MTE specific settings after a restart, keep the SAP system components up-to-date by using the correct Kernel and support package patch level.



# Chapter 83: SAP CCMS Alerts Monitor

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.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of SAP monitoring. For details, see SAP Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP CCMS monitor.

## Learn About

### Supported Platforms/Versions

This monitor enables supports monitoring 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.

### License Consumption

Points-based Usage	Capacity-based Usage
1 point per metric	One OSi license per monitored host Note: Not available with Community Edition.

## Tasks

### How to Configure the SAP Alerts CCMS Monitor

#### 1. Prerequisites

- Before configuring the monitor, make sure you have the necessary setup requirements and user privileges to log on to the CCMS server and retrieve metrics.
  - The SAP Java Connector (SAP JCo 3.x) component must be installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location). For details, see step 3 below.
  - The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and later only.
  - You must have SAP authorization of the remote system user. For details on the SAP permissions required by SiteScope, see ["SAP Permissions" on the next page](#).
  - Consult your SAP documentation to determine if your R/3 landscape components requires additional software installed to run or work with CCMS.

- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries.

## 2. SAP Permissions

- The following is the minimal set of SAP authorizations required by SiteScope in order to create and retrieve the necessary data from the monitor:

RFC1, SALX, SDIF\*, SXMI, SYST, SYSU

S_RFC – Authorization check for RFC access	
Activity	16 (Execute)
Name of RFC to be protected	SXMI, SALX, SYST
Type of RFC object to be protected	FUGR

- Alternatively, you can set certain privileges for SAP user 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 log on 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 user interface and see if the CCMS monitor sets can be displayed.

## 3. Download the SAP Java Connector

The SAP 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.

Download and install the SAP Java Connector 3.x component to the server where SiteScope is running (or at least it must be accessible on a shared or remote location).

- a. Log on 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. After you log on, select **SAP NetWeaver > SAP NetWeaver in Detail > Application Platform > Connectivity > Connectors > SAP Java Connector**, and then click **Tools and Services**.
- c. Before downloading JCo 3.x.jar and .dll files, you must perform the following:
  - Remove any previously installed **sapjco.jar** files before downloading the JCo 3.x files.
  - Set the **SAP Java Connector version** property in **Preferences > Infrastructure Preferences > Monitor Settings** to **3.x**.
- d. Download the JCo 3.x.jar and .dll files from the SAP support Web site:  
On a Windows environment, download:

File	Copy to...
sapjco3.jar	<SiteScope root directory>\WEB-INF\lib
sapjco3.dll	<SiteScope root directory>\bin

On a UNIX environment, download:

File	Copy to...
sapjco3.jar	<b>&lt;SiteScope root directory&gt;/WEB-INF/lib</b> <b>Note:</b> JCO native libraries must be copied to <b>/usr/lib64</b> . To check that a JCO connector is installed correctly, run the following command: <code>/opt/HP/SiteScope/java/bin/java -jar /opt/HP/SiteScope/WEB-INF/lib/sapjco3.jar</code>
libsapjco3.so	<ul style="list-style-type: none"> <li>For Sun installations: <b>&lt;SiteScope root directory&gt;/java/lib/sparc</b></li> <li>For Linux installations: <b>/usr/lib64</b></li> </ul>

e. Restart SiteScope.

#### 4. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Note:** Although you can change the run schedule for this monitor using the **Frequency** setting in Monitor Run Settings (the default is every 10 minutes), CCMS metrics are generally only updated once every 5 minutes.

## UI Descriptions

### SAP CCMS Alerts Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Application server</b>	Host name/IP address of the SAP server you want to monitor.
<b>SAP client</b>	Client to use for connecting to SAP.
<b>System number</b>	System number for the SAP server.

UI Element	Description
<b>SAP router string</b>	<p>Router address string if your connection is being made through a router (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>Option for providing the user name and password 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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p>
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For details, see <a href="http://help.sap.com/saphelp_erp60_sp/helpdata/en/f0/4f70403590ca01e10000000a155106/frameset.htm">http://help.sap.com/saphelp_erp60_sp/helpdata/en/f0/4f70403590ca01e10000000a155106/frameset.htm</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 84: SAP Java Web Application Server Monitor

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.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of SAP monitoring. For details, see SAP Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP Java Web Application Server monitor.

## Learn About

### Supported Platforms/Versions

This monitor supports monitoring:

- SAP Java Web Application Server 6.40, 7.00, 7.01, 7.02, 7.3
- SAP Enterprise Portal 5.0, 6.0
- SAP NetWeaver Portal 7.0, 7.3

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host
	Note: Monitor is not available when using Community edition.

## Tasks

### How to Configure the SAP Java Web Application Server Monitor

#### 1. Prerequisites

- This monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running.
- You must have SAP authorization of the remote system user. For details on the SAP permissions required by SiteScope, see ["SAP Permissions" on the next page](#).

- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries
- The SAP Java Web Application Server monitor uses SAP JMX Connector libraries to connect to SAP J2EE cluster. Depending on your monitored environment, the JMX Connector files are available on the SAP Java Web Application server from `\usr\sap\<SID>\JC\<InstanceNumber>\j2ee\admin\lib` or `\usr\sap\<SID>\DVEBMGS\<InstanceNumber>\j2ee\admin\lib`.
  - i. 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**
    - **logging.jar**
    - **jmx.jar**
  - ii. Restart SiteScope
- To enable monitoring a SAP Java Web Application Server 6.40 or 7.00-7.02 server, you must install a patch (SAP Note 1740150) from the SAP portal ([https://websmp230.sap-ag.de/sap\(bD1lbiZjPTAwMQ==\)/bc/bsp/spn/sapnotes/index2.htm?numm=1740150](https://websmp230.sap-ag.de/sap(bD1lbiZjPTAwMQ==)/bc/bsp/spn/sapnotes/index2.htm?numm=1740150)). The SAP JMX Client jars should be taken from the patched SAP system.

For versions SAP NetWeaver 7.1.1 and higher, the following JMX client jars should be copied from `\usr\sap\I30\DVEBMGS00\j2ee\j2eeclient` on the SAP Java Web Application server:

- **sap.com~tc~exception~impl.jar**
- **sap.com~tc~je~clientlib~impl.jar**
- **sap.com~tc~je~leanClient.jar**
- **sap.com~tc~logging~java~impl.jar**
- **tc~bl~base~client.jar**
- **tc~bl~deploy~client.jar**

## 2. SAP Permissions

The following is the minimal set of SAP authorizations required by SiteScope in order to create and retrieve the necessary data from the monitor,

- You need to create a SAP role with one assigned action:
  - Type: **UME**
  - Service / Application: **tc~pi~monitor~perm**
  - Name: **PI\_PAYLOAD\_MONI**

and then assign it to a SAP user.

- Alternatively, you can use the predefined **SAP\_XI\_PCK\_MONITOR** role that contains the above-listed action (and others).

## 3. Enable monitoring the P4 port using a secure connection - optional

- a. Copy the jar files from the `usr\sap\<INSTANCE_NAME>\SYS\global\security\lib\tools` directory on the SAP machine into the **<SiteScope root directory>\WEB-INF\lib** directory.

- b. When setting the monitor properties (in the following step), configure the following:
  - **Port.** Enter the port number that allows P4 over SSL connections. For details on J2EE port requirements, see [https://help.sap.com/saphelp\\_nw70ehp1/helpdata/en/a2/f9d7fed2adc340ab462ae159d19509/content.htm](https://help.sap.com/saphelp_nw70ehp1/helpdata/en/a2/f9d7fed2adc340ab462ae159d19509/content.htm).
  - **Transport layer:** Select **SSL**.

#### 4. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### SAP Java Web Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Application server</b>	Address of the SAP Java Web Application Server you want to monitor.
<b>Port</b>	Number of the P4 port for the SAP Java Web Application Server you want to monitor. For details on J2EE port requirements, see <a href="https://help.sap.com/saphelp_nw70ehp1/helpdata/en/a2/f9d7fed2adc340ab462ae159d19509/content.htm">https://help.sap.com/saphelp_nw70ehp1/helpdata/en/a2/f9d7fed2adc340ab462ae159d19509/content.htm</a> . <b>Default value:</b> 50004
<b>Transport layer</b>	Select the option for monitoring the P4 port. <ul style="list-style-type: none"><li>• <b>SSL.</b> Select this option to monitor P4 using a secure SSL transport layer connection.</li><li>• <b>No underlying transport layer.</b> Select this option to use a non-secure connection.</li></ul>
<b>Credentials</b>	Option for providing the user name and password 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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>Counters</b>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.

UI Element	Description
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. These counters are received dynamically from the JMX.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.



# Chapter 85: SAP MAI Alert Monitor

The SAP MAI Alert monitor retrieves and reports alerts and its sub objects from the SAP Solution Manager and displays the counters. The counters that are displayed are dynamic in nature and depend on the alerts triggered on the Solution Manager when the SiteScope monitors are running.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP MAI Alert monitor.

## Learn About

This section includes:

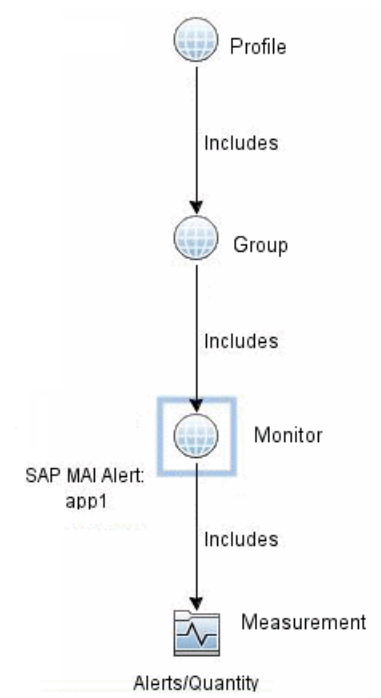
- ["Supported Platforms/Versions" below](#)
- ["SAP MAI Alert Topology" below](#)
- ["License Consumption" on the next page](#)

## Supported Platforms/Versions

This monitor supports monitoring on SAP Solution Manager 7.1.

## SAP MAI Alert Topology

The SAP MAI Alert monitor can identify the topology of the SAP Solution Manager being monitored. The monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM as SiteScope Measurement Groups and SiteScope Measurement CIs.

**Note:**

- This direct integration between SiteScope and BSM is available only when the Application Management for SAP license is installed.
- When you add a new application server to the SAP System, you must clear the **Report monitor and related CI topology** 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 details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Report Discovered Topologies to BSM in the Using SiteScope Guide.

For information about the SAP topology, see SAP Systems View in the BSM User Guide in the BSM Help.

## License Consumption

Points-based Usage	Capacity-based Usage
50 points per monitor	One OSi license per monitored host
	Note: Monitor is not available when using Community edition.

# Tasks

## How to Configure the SAP MAI Alert Monitor

### 1. Prerequisites

Before configuring the monitor, make sure you have the necessary setup requirements and user privileges to log on to the SAP Solution Manager and retrieve counters.

- You must have SAP authorization of the remote system user. For details on the SAP permissions required by SiteScope, see ["SAP Permissions" below](#).
- The SAP Java Connector (SAP JCo 3.x) component must be installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location). For details, see step 3 below.
- Copy the transport file provided by SiteScope to the transport directories on SAP Solution Manager. For steps to apply the transports, see ["Apply the SAP Transport" on page 564](#).
- Configure the SAP Solution Manager for activating the alert reaction Business Add Ins (BADI). For steps to configure, see ["Configure SAP Solution Manager for activating the alert reaction BADI" on page 565](#)
- Consult your SAP documentation to determine if your SAP Solution Manager requires any additional software.

### 2. SAP Permissions

The following is the minimal set of SAP authorizations required by SiteScope to create and retrieve the necessary data from the monitor:

<b>S_RFC – Authorization check for RFC access</b>	
Activity	All activities
Name of RFC to be protected	/HPOV/*
Type of RFC object to be protected	All values

### 3. Download the SAP Java Connector

The SAP 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.

Download and install the SAP Java Connector 3.x component to the server where SiteScope is running (or at least it must be accessible on a shared or remote location).

- a. Log on 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. After you log on, select **SAP NetWeaver > SAP NetWeaver in Detail > Application Platform > Connectivity > Connectors > SAP Java Connector**, and then click **Tools and Services**.
- c. Before downloading JCo 3.x.jar and .dll files, you must perform the following:
  - Remove any previously installed **sapjco.jar** files before downloading the JCo 3.x files.
  - Set the **SAP Java Connector version** property in **Preferences > Infrastructure Preferences > Monitor Settings** to **3.x**.
- d. Download the JCo 3.x.jar and .dll files from the SAP support Web site:

On a Windows environment, download:

File	Copy to...
sapjco3.jar	<SiteScope root directory>\WEB-INF\lib
sapjco3.dll	<SiteScope root directory>\bin

On a UNIX environment, download:

File	Copy to...
sapjco3.jar	<b>&lt;SiteScope root directory&gt;/WEB-INF/lib</b> <b>Note:</b> JCO native libraries must be copied to <b>/usr/lib64</b> . To check that a JCO connector is installed correctly, run the following command: <pre>/opt/HP/SiteScope/java/bin/java -jar /opt/HP/SiteScope/WEB-INF/lib/sapjco3.jar</pre>
libsapjco3.so	<ul style="list-style-type: none"> <li>◦ For Sun installations: <b>&lt;SiteScope root directory&gt;/java/lib/sparc</b></li> <li>◦ For Linux installations: <b>/usr/lib64</b></li> </ul>

- e. Restart SiteScope.

#### 4. Apply the SAP Transport

To copy the SAP transport files to the SAP Solution Manager, follow these steps:

- a. Use the Windows Explorer tool to locate the SAP transport packages, which are available by default in the following directory on the SiteScope server:

For Windows: **<SiteScope root directory>\sitescope\_SAPMAI\_transport\SAP\_Trans\_HPSiteScope.car**

For Linux: **/opt/HP/SiteScope/sitescope\_SAPMAI\_transport/SAP\_Trans\_HPSiteScope.car**

- b. Use the ftp method to transfer the package to the SAP Solution Manager instance.
- c. Log on as a SAP administrator (<SID>adm) on the SAP instance, and use the CAR (or SAPCAR) command to unpack the transport files to /usr/sap/trans. Type the following command:  
CAR -xvf SAP\_Trans\_HPSiteScope.car
- d. You can import the SAP transport either by using command line or SAP GUI.

- o To import using the command prompt, follow these steps:

Import the SAP transport to your SAP Solution Manager instance. Enter the following commands as SAP administrator (<SID>adm) on the managed node:

```
cd \usr\sap\trans\bin
```

```
tp addtobuffer <transport_file_name> <SID>
```

```
tp import <transport_file_name> <SID> client=<client_number>
```

The required transports are:

- SM4K900030 – HP SiteScope for SAP Solution Manager 7.1 – Main Transport
- SM4K900028 – HP SiteScope for SAP Solution Manager 7.1 – User role

In this example, <SID> is the SAP system ID and <transport\_file\_name> is the name of the transport file, which corresponds to the version of SAP running on the SiteScope managed node.

If you encounter errors when using the tp addtobuffer command, you can clean the tp buffer using the following command:

```
tp cleanbuffer <SID>
```

- o Alternatively, you can import transport files using the SAP GUI. To import transport files using the SAP GUI, follow these steps:
    - A. Log on to the SAP Solution Manager where you want to apply the SAP transport file.
    - B. In the SAP GUI, enter the following transaction ID to display the SAP Transport Management System (SMTS) login page: STMS
    - C. In the SAP Transport Management System login page, click the **Transport** icon (or press the F5 function key).
    - D. Select the SID of the SAP System into which you want to import the SiteScope for SAP transport.
    - E. In the file menu, click **Extras > Other requests > Add**.
    - F. In the Transport-Request-to-Import queue, enter the following:  
<Transport\_file\_name>
    - G. Select the **Check [✓]** icon or use the **Enter** key to add transaction requests.


- H. Highlight the required transport. The required transports are as follows:
  - SM4K900030 – HP SiteScope for SAP Solution Manager 7.1 – Main Transport
  - SM4K900028 – HP SiteScope for SAP Solution Manager 7.1 – User role
- I. Select **Request > Import**. The Import Request dialog box opens.
- J. Enter the target client number (000 is the default client number).
- K. Check items in the Option tab that are appropriate for your system.
- L. Click the **Check [✓]** icon or press **Enter**.
- M. Repeat this procedure for each SAP Solution Manager that you want to manage with SiteScope.

## 5. Configure SAP Solution Manager for activating the alert reaction BADI

To configure the technical alert reaction BADI, follow these steps:

- a. Log on to Solution Manager as an administrator.
- b. Open the solman\_setup transaction.
- c. Select **Technical Monitoring > System Monitoring**. The System Monitoring dialog opens.
- d. Select **2: Configure Infrastructure > 2.3: Default Settings** and select **Third-Party Components** tab.
- e. Click **Add** and select the option **BADI for reacting to MAI Alerts and extracting the Alert/Event/Metric details**.
- f. In the **Scope Filter** box, select **All Alerts, Events and Metrics (without Internal Events)**.
- g. Select **5: Define Scope** and select the managed objects from the list of **Technical Systems**.
- h. Click **Next** and select **Apply and Activate > All managed objects**. After activation, the status of the selected managed objects show green in the setup status column.
- i. Exit the solman\_setup transaction.


## 6. Configure the monitor properties

- a. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions below.
- b. For dynamic monitoring, add patterns to counters to instruct the monitor which counters to use. Click the **Add New Counter**  button to add an empty line to the table, and then create a pattern format using a regular expression.

### Tip:

- The pattern should always start and end with the forward slash ("/") character.
- The "[" and "]" characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character)
- Use "." to describe any character any number of times.

For example, /java.lang/Memory/.\*/ shows all memory counters that are exposed by the java.lang domain.

- c. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counter Preview tree.
- d. Set the frequency for updating counters from the server, and then click **Verify & Save** or **Save** to

save your settings.

- e. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

## 7. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["SAP MAI Alert Topology" on page 561](#).




For user interface details, see BSM Integration Data and Topology Settings in the Using SiteScope Guide.

# UI Descriptions

## SAP MAI Alert Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Application server</b>	Host name/IP address of the SAP server you want to monitor.
<b>SAP client</b>	Client to use for connecting to SAP.
<b>System number</b>	System number of the SAP server.
<b>SAP router string</b>	<p>Router address string if your connection is being made through a router (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>Option for providing the user name and password to access the SAP MAI counters:</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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>

UI Element	Description
<b>Patterns &amp; Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to view the available counters.</p> <p>Click the <b>Add New Counter</b>  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the <b>Delete Counter</b>  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the <b>View Matches for Selected Pattern Counter</b>  button to display counters that match the selected patterns.</p>
<b>Get Counters</b>	<p>Opens the Select Counters Form to view the counters you want to monitor. For details, see <a href="http://help.sap.com/saphelp_erp60_sp/helpdata/en/f0/4f70403590ca01e10000000a155106/frameset.htm">http://help.sap.com/saphelp_erp60_sp/helpdata/en/f0/4f70403590ca01e10000000a155106/frameset.htm</a>.</p> <p>Note: Do <b>not</b> select the counters from the counter tree in the Select Counters Form. You must add patterns to counters to instruct the monitor which counters to use.</p>
<b>Continue displaying counters that no longer exist after update</b>	<p>This option is not available for this monitor. Selecting the option does not have any impact. This option will be removed in the next version of SiteScope.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and tips for the SAP MAI Alert monitor.

### General Notes/Limitations

- **Error getting counters: unable to retrieve the counters**  
Verify you have the required .jar and .dll/.so files to configure the SAP MAI Alert monitor as listed in "Prerequisites" on page 562.
- **Dashboard displays counter summary as Alerts/Quantity = 0.**  
There are no alerts available in the SAP Solution Manager during the monitor run time.

# Chapter 86: SAP Performance Monitor

Use the SAP Performance monitor to monitor the server and database performance data for SAP Application Servers. 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. The error and warning thresholds for the monitor can be set on SAP server and database performance statistics.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of SAP monitoring. For details, see SAP Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP Performance monitor.

## Learn About

### Supported Platforms/Versions

This monitor supports monitoring SAP Application Servers R/3 4.6B, R/3 4.6C, R/3 4.7E, SAP ECC5 and SAP ECC6.

### License Consumption

Point-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitor Note: Monitor is not available when using Community edition.

## Tasks

### How to Configure the SAP Performance Monitor

#### 1. Prerequisites

- The SAP Java Connector (SAP JCo 3.x) component must be installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location). For details, see step 3 below.
- You must have SAP authorization of the remote system user. For details on the SAP permissions required by SiteScope, see ["SAP Permissions" on the next page](#).
- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries.



## 2. SAP Permissions

- The following is the minimal set of SAP authorizations required by SiteScope in order to create and retrieve the necessary data from the monitor:

RFC1, SALX, SDIF\*, SXMI, SYST, SYSU, STUM, SAPWL\_GLOB\_STAT, STD1, STUS, SVRZ

S_RFC – Authorization check for RFC access	
Activity	16 (Execute)
Name of RFC to be protected	SXMI, SALX, SYST
Type of RFC object to be protected	FUGR

- Alternatively, 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

One test to see if a user has such authorization is to try and issue transaction RZ20 in the SAP user interface and see if the CCMS monitor sets can be displayed.

## 3. Download the SAP Java Connector

The SAP 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.

Download and install the SAP Java Connector 3.x component to the server where SiteScope is running (or at least it must be accessible on a shared or remote location).

- Log on 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

- After you log on, select **SAP NetWeaver > SAP NetWeaver in Detail > Application Platform > Connectivity > Connectors > SAP Java Connector**, and then click **Tools and Services**.
- Before downloading JCo 3.x.jar and .dll files, you must perform the following:
  - Remove any previously installed **sapjco.jar** files before downloading the JCo 3.x files.
  - Set the **SAP Java Connector version** property in **Preferences > Infrastructure Preferences > Monitor Settings** to **3.x**.
- Download the JCo 3.x.jar and .dll files from the SAP support Web site:

On a Windows environment, download:

File	Copy to...
sapjco3.jar	<SiteScope root directory>\WEB-INF\lib
sapjco3.dll	<SiteScope root directory>\bin

On a UNIX environment, download:

File	Copy to...
sapjco3.jar	<b>&lt;SiteScope root directory&gt;/WEB-INF/lib</b> <b>Note:</b> JCO native libraries must be copied to <b>/usr/lib64</b> . To check that a JCO connector is installed correctly, run the following command: <pre>/opt/HP/SiteScope/java/bin/java -jar /opt/HP/SiteScope/WEB-INF/lib/sapjco3.jar</pre>
libsapjco3.so	<ul style="list-style-type: none"> <li>For Sun installations:  <b>&lt;SiteScope root directory&gt;/java/lib/sparc</b> </li> <li>For Linux installations:  <b>/usr/lib64</b> </li> </ul>

e. Restart SiteScope.

#### 4. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### SAP Performance Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Application server</b>	Address of the SAP server you want to monitor.
<b>SAP client</b>	Client to use for connecting to SAP.
<b>System number</b>	System number for the SAP server.
<b>SAP router string</b>	<p>Router address string if your connection is being made through a router (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>

UI Element	Description
<b>Credentials</b>	<p>Option for providing the user name and password 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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p>
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<p><b>Database performance (Oracle)</b></p> <ul style="list-style-type: none"> <li>• Calls - Parses</li> <li>• Calls - Reads / User calls</li> <li>• Calls - Recursive calls</li> <li>• Calls - User calls</li> <li>• Calls - User/Recursive calls</li> <li>• Calls - commits</li> <li>• Calls - rollbacks</li> <li>• Data buffer - Buffer busy waits</li> <li>• Data buffer - Buffer wait time s</li> <li>• Data buffer - Physical reads</li> <li>• Data buffer - Quality</li> <li>• Data buffer - Reads</li> <li>• Data buffer - Size kb</li> <li>• Data buffer - writes</li> <li>• Log buffer - Alloc fault rate</li> <li>• Log buffer - Allocation retries</li> <li>• Log buffer - Entries</li> <li>• Log buffer - Log files (in use)</li> <li>• Log buffer - Redo log waits</li> <li>• Log buffer - Size kb</li> <li>• Redo logging - Latching times</li> <li>• Redo logging - Mb written</li> <li>• Redo logging - OS-Blocks written</li> <li>• Redo logging - Write times</li> <li>• Redo logging - Writes</li> <li>• Shared Pool - DD-Cache quality</li> <li>• Shared Pool - SQL Area get ratio</li> <li>• Shared Pool - Size kb</li> <li>• Shared Pool - pin ratio %</li> <li>• Shared Pool - reloads/pins</li> <li>• Sorts - Disk</li> <li>• Sorts - Memory</li> <li>• Sorts - Rows sorted</li> <li>• Table scans &amp; fetches - Fetch by row id</li> <li>• Table scans &amp; fetches - Long table scans</li> <li>• Table scans &amp; fetches - Short table scans</li> <li>• Table scans &amp; fetches - by continued row</li> </ul>	<ul style="list-style-type: none"> <li>• Time statistics - Busy wait times</li> <li>• Time statistics - CPU count</li> <li>• Time statistics - CPU times</li> <li>• Time statistics - CPU usage %</li> <li>• Time statistics - Sessions busy %</li> <li>• Time statistics - Time/User call ms</li> </ul> <p><b>Database performance (MSSQL)</b></p> <ul style="list-style-type: none"> <li>• Memory Usage/Current memory kb</li> <li>• Memory Usage/Maximum memory kb</li> <li>• Memory Usage/Procedure cache kb</li> <li>• Memory Usage/Procedure cache hit ratio %</li> <li>• Memory Usage/Total SQL connections</li> <li>• Memory Usage/Free pages</li> <li>• Memory Usage/Data cache size kb</li> <li>• Memory Usage/Data cache hit ratio %</li> <li>• Space Usage/Total data size Mb</li> <li>• Space Usage/Free Space Mb</li> <li>• Space Usage/Total log size Mb</li> <li>• Space Usage/Free space Mb</li> <li>• Server Engine/CPU busy s</li> <li>• Server Engine/CPU idle s</li> <li>• Server Engine/IO busy s</li> <li>• Server Engine/Physical reads</li> <li>• Server Engine/Physical writes</li> <li>• Server Engine/Physical errors</li> <li>• Workload/CPU Time</li> <li>• Workload/Dialog steps</li> <li>• Workload/Average CPU time</li> <li>• Workload/Av. RFC+CPIC time</li> <li>• Workload/Av. response time</li> <li>• Workload/Average wait time</li> <li>• Workload/Average load time</li> <li>• Workload/Av. Roll i+w time</li> <li>• Workload/Av. DB req. time</li> <li>• Workload/Av. enqueue time</li> <li>• Workload/Database requests</li> <li>• SQL Requests/SQL batches</li> </ul>	<ul style="list-style-type: none"> <li>• SQL Requests/Read ahead pages</li> <li>• SQL Requests/Request buffer pages</li> <li>• SQL Requests/Request buffer reads</li> <li>• SQL Requests/Request buffer writes</li> <li>• Workload/Roll-in time</li> <li>• Workload/Roll-out time</li> <li>• Workload/Roll wait time</li> <li>• Workload/Roll-ins</li> <li>• Workload/Roll-outs</li> </ul> <p><b>Workload</b></p> <ul style="list-style-type: none"> <li>• Av. DB req. time</li> <li>• Av. enqueue time</li> <li>• Av. response time</li> <li>• Av. RFC+CPIC time</li> <li>• Av. Roll i+w time</li> <li>• Average bytes req.</li> <li>• Average CPU time</li> <li>• Average load time</li> <li>• Average wait time</li> <li>• CPU Time</li> <li>• Database calls</li> <li>• Database requests</li> <li>• DB Calls: Changes</li> <li>• DB Calls: Direct reads</li> <li>• DB Calls: Sequential reads</li> <li>• Dialog steps</li> <li>• Roll wait time</li> <li>• Roll-in time</li> <li>• Roll-ins</li> <li>• Roll-out time</li> <li>• Roll-outs</li> <li>• Time per DB request</li> <li>• Time per Req.: Changes and commits</li> <li>• Time per Req.: Direct reads</li> <li>• Time per Req.: Sequential reads</li> </ul>
---	---	--

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 87: SAP Work Processes Monitor

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.

Using the SAP Work Processes monitor, you can also enable reporting of the host topology to BSM. If enabled, BSM automatically populates the RTSM with CIs based on the monitored hardware in SiteScope.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of SAP monitoring. For details, see SAP Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SAP Work Processes monitor.

## Learn About

This section contains the following topics:

- ["Understanding the SAP Work Processes Monitor" below](#)
- ["Supported Platforms/Versions" below](#)
- ["SAP Work Processes Topology" on the next page](#)
- ["License Consumption" on the next page](#)

## 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.

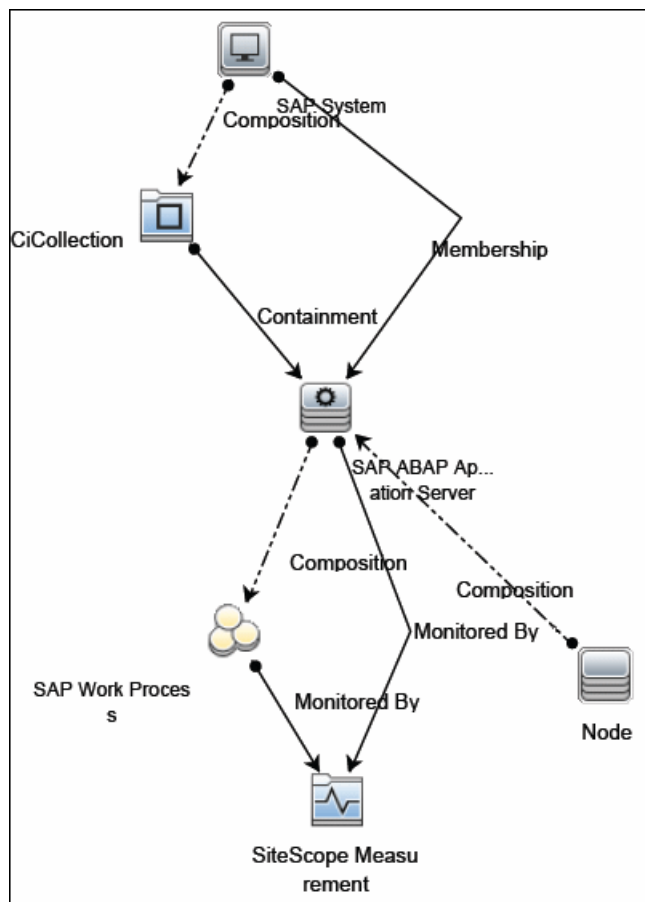
The dispatcher assigns tasks to the free work processes, making optimal use of system resources and balancing the system load. The dispatcher knows and distributes pending tasks according to the type of the defined processes. The difference among the various work processes affects only those tasks or special services that have been assigned to the work processes through the dispatching strategy.

## Supported Platforms/Versions

This monitor supports monitoring SAP Application Servers R/3 4.6B, R/3 4.6C, R/3 4.7E, SAP ECC5 and SAP ECC6.

## SAP Work Processes Topology

The SAP Work Processes monitor can identify the work processes of the server being monitored. The monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM as SiteScope Measurement Groups and SiteScope Measurement CIs.

**Note:** This direct integration between SiteScope and BSM is available only when the Application Management for SAP license is installed.

For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

For information about the SAP topology, see SAP Systems View in the BSM User Guide in the BSM Help.

## License Consumption

Point-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitor
	Note: Monitor is not available when using Community edition.

# Tasks

## How to Configure the SAP Work Processes Monitor

### 1. Prerequisites

- The SAP Java Connector (SAP JCo 3.x) component must be installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location). For details, see step 3 below.
- You must have SAP authorization of the remote system user. For details on the SAP permissions required by SiteScope, see "[SAP Permissions](#)" below.
- The **compat-libstdc++** package is required for Amazon Linux to resolve dependencies between SAP and Amazon Linux system libraries.

### 2. SAP Permissions

- The following is the minimal set of SAP authorizations required by SiteScope in order to create and retrieve the necessary data from the monitor:

RFC1, SALX, SDIF\*, SXMI, SYST, SYSU, SMON, STUM

S_RFC – Authorization check for RFC access	
Activity	16 (Execute)
Name of RFC to be protected	SXMI, SALX, SYST
Type of RFC object to be protected	FUGR

- Alternatively, 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

### 3. Download the SAP Java Connector

The SAP 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.

Download and install the SAP Java Connector 3.x component to the server where SiteScope is running (or at least it must be accessible on a shared or remote location).

- a. Log on 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. After you log on, select **SAP NetWeaver > SAP NetWeaver in Detail > Application Platform > Connectivity > Connectors > SAP Java Connector**, and then click **Tools and Services**.



- c. Before downloading JCo 3.x.jar and .dll files, you must perform the following:
  - Remove any previously installed **sapjco.jar** files before downloading the JCo 3.x files.
  - Set the **SAP Java Connector version** property in **Preferences > Infrastructure Preferences > Monitor Settings** to **3.x**.

- d. Download the JCo 3.x.jar and .dll files from the SAP support Web site:

On a Windows environment, download:

File	Copy to...
sapjco3.jar	<SiteScope root directory>\WEB-INF\lib
sapjco3.dll	<SiteScope root directory>\bin

On a UNIX environment, download:

File	Copy to...
sapjco3.jar	<b>&lt;SiteScope root directory&gt;/WEB-INF/lib</b>  <b>Note:</b> JCO native libraries must be copied to <b>/usr/lib64</b> . To check that a JCO connector is installed correctly, run the following command:  <code>/opt/HP/SiteScope/java/bin/java -jar /opt/HP/SiteScope/WEB-INF/lib/sapjco3.jar</code>
libsapjco3.so	<ul style="list-style-type: none"><li>◦ For Sun installations: <b>&lt;SiteScope root directory&gt;/java/lib/sparc</b></li><li>◦ For Linux installations: <b>/usr/lib64</b></li></ul>

- e. Restart SiteScope.

#### 4. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

#### 5. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["SAP Work Processes Topology" on page 575](#).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

# UI Descriptions

## SAP Work Processes Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Application server</b>	Address of the SAP server you want to monitor.
<b>SAP client</b>	Client to use for connecting to SAP.
<b>System number</b>	System number for the SAP server.
<b>SAP router string</b>	<p>Router address string if your connection is being made through a router (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>Option for providing the user name and password 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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>Counters</b>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.

UI Element	Description
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. You can configure the following counters for this monitor:</p> <p>Counts work processes in the following categories:</p> <ul style="list-style-type: none"><li>• All</li><li>• Dialog</li><li>• Update</li><li>• Background</li><li>• Enqueue</li><li>• Spool</li></ul> <p>Reports the following counters for each category:</p> <ul style="list-style-type: none"><li>• Total number of WP</li><li>• Number of waiting</li><li>• Number of running</li><li>• Number of stopped</li><li>• Number of other</li><li>• Max CPU in this category</li><li>• Max memory</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 88: Script Monitor

This monitor enables you to integrate existing system management scripts into the SiteScope environment by running external commands and reporting the command result. It also enables you to parse and report a specific value from the command output.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Script monitor.

## Learn About

This section includes:

- ["Script Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Script Options" on the next page](#)
- ["Status" on page 582](#)
- ["Caching Script Output" on page 582](#)
- ["Setting a Timeout Value for Script Execution" on page 582](#)
- ["Running Different Types of Scripts" on page 583](#)
- ["Script Return Status Example" on page 583](#)
- ["License Consumption" on page 584](#)

## 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 if this monitor was in error.

Symbolic links are now supported when executing scripts on remote UNIX servers. This support is enabled by changing the **Script monitor allow symbolic link** property in **Preferences > Infrastructure Preferences > Custom Settings** to **true**. When enabled, the symbolic link appears in the list of available scripts when configuring a Script monitor to monitor a UNIX remote.

**Note:** SiteScope Failover does not support copying of symbolic links.

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using

Secure Shell (SSH) in the Using SiteScope Guide.

- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- The Script monitor supports monitoring remote servers running on HP NonStop operating systems. For details on enabling the HP NonStop operating system monitoring environment, see ["How to Configure the HP NonStop Resources Monitor" on page 307](#).

## 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 <b>&lt;SiteScope root directory&gt;\scripts</b> 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></p> <ul style="list-style-type: none"> <li>• On Window platforms, the path to the user home directory depends on the particular SSH server. For example if you install a Cygwin SSH server in C:\Cygwin, the default path to the home directory for the Administrator user will be C:\Cygwin\home\Administrator. For additional information, see the documentation for your SSH server.</li> <li>• Only executable script files are displayed.</li> </ul> <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 help echo end script</pre>
Remote Command	A script file containing a single command stored locally in the <b>&lt;SiteScope root directory&gt;\scripts.remote</b> 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 ["Script Return Status Example" on the next page](#) 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 584](#).

## Running Different Types of Scripts

You can run non-batch scripts, for example VBScript or Perl scripts, without wrapping them into a batch file.

**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 by adding the **\_scriptMonitorExtensions** 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 specifying the **\_scriptInterpreters** property in the **master.config** file as follows: `_scriptInterpreters=pl=c:/perl/perl.exe;py=c:/python/python.exe;php=c:/php/php.exe`

## Script Return Status Example

To get around the fact that exit codes that are not returned to SiteScope after execution of Win NT batch files or UNIX scripts executed on remote servers, we recommend including an echo to standard out of a return value. In the case of Win NT-to-NT remote scripts (using Secure Shell), the remote script must echo end script when the script has terminated. Other returned values can then be matched in the Script monitor using a regular expression in the Match expression box.

In the script that runs on a remote server, include echo commands that represent the different logical paths that might be followed. The following is an example script outline based on a UNIX shell script:

```
#!/bin/sh
...(script commands and logic here)...
echo "Return Code: 1" (indicating the script failed to complete execution)
...(more script commands and logic here)...
echo "Return Code: 0" (the end of the script, indicating the script completed successfully)
```

In the **Match expression** box, enter the following regular expression pattern:

```
/Return Code: (\d+)/
```

Then set the Error, Warning, and Good thresholds for the monitor as follows:

**Error if** value > 0

**Warning if** value == 'n/a'

**Good if** value == 0

With this set up, there are 2 possible outcomes:

- **echoed Return Code value is greater than 0.** This indicates that the script did not execute correctly. If the script does not run properly, meaning that no Return Code echo command in the script is executed, then a warning condition occurs (for example, there is no match for the Match Expression that returns **n/a**).
- **echoed Return Code of 0.** This indicates that a good condition is detected. The monitor status shown on the Monitor Detail page displays **matched 0** if the script executed successfully.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor up to 4 pattern match metrics; above this, 1 point per additional pattern match metric, that is, #OfMatchValueMetrics-3.	One OSi license per monitored host

## Tasks

### How to Configure the Script Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.

**Note:** The Script monitor should be used carefully to avoid accidentally or maliciously damaging the target remote machine on which the script runs. We recommend using this monitor on remote servers that have strong security only.

2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Script Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of 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 using SSH are displayed).</p> <p>To monitor ILOM SSH login, select a UNIX remote configured to use a Sun Fire X64 ILOM operating system.</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>



UI Element	Description
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Script</b>	<p>The script to run. SiteScope gets scripts from a scripts subdirectory in the home directory of the account SiteScope uses to access the remote server. For example, <code>home/sitescope/scripts</code>. On Windows, SiteScope gets scripts from the home directory on the remote machine (this depends on the SSH server configuration). For example, <code>C:\Documents and Settings\Administrator\Scripts</code> directory.</p> <p>When monitoring the SiteScope Server, 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>Syntax exception:</b> Do not include any command that would normally discontinue script processing (for example, do not use the <code>exit</code> command).</p>
<b>Reload Scripts</b>	Reloads the selected monitor scripts.
<b>Parameters</b>	<p>Specifies any additional parameters to pass to the script. You can use a regular expression or use the attributes found in SiteScope alert templates to insert variables into the parameters box. For details, see SiteScope Alert Template and Event Properties Directory.</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: <code>` ; &amp;  </code></p>

UI Element	Description
<b>Output encoding</b>	<p>Select the code page or encoding to use if the command output uses an encoding that is different than the encoding used on the server where SiteScope is running. 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>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>
<b>Match expression</b>	<p>Regular expression used to retrieve values from the script output. For example, the expression: <code>/(\d+)/</code> matches one or more digits returned by the script. Use parentheses to enable 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>
<b>Open Tool</b>	<p>Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.</p>

UI Element	Description
<b>Remote script command file</b>	<p>The script file that contains the commands that SiteScope should send to the remote machine if you USE COMMAND is selected as the Script option and a remote machine as the Server. You can save one or more commands in the text script file and save the file in the <b>&lt;SiteScope root directory&gt;\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 <code>exit</code> command).</p>
<b>Cache life (seconds)</b>	<p>Uses 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>
<b>Measurement maximum (milliseconds)</b>	<p>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>
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, to wait for the script to run successfully before timing out.</p> <p><b>Default value:</b> -1 (no timeout)</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons

are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

- 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'.
- The Script monitor **round trip time** counter includes SiteScope server loading time, such as time required for preparing the monitor run, the network transfer, and script execution. The **script execution time** counter shows the time spent for running the script (it is preferable to use this counter for script performance diagnostics than the **round trip time** counter).
- The Script monitor should be used carefully to avoid accidentally or maliciously damaging the target remote machine on which the script runs. We recommend using this monitor on remote servers that have strong security only.

# Chapter 89: Service Monitor

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Service monitor.

## Learn About

This section includes:

- ["Service Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Status" on the next page](#)
- ["Scheduling the Monitor" on the next page](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)
- ["License Consumption" on the next page](#)

## Service Monitor Overview

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.

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 if your monitor fails. For details on using a Script Alert, see Working with Script Alerts in the Using SiteScope Guide.

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows platforms and on UNIX versions if the remote server being monitored has been configured for SSH. For details, see SiteScope Monitoring Using Secure Shell (SSH) in the Using SiteScope Guide.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2 Update 1.
- This monitor supports WMI (Windows Management Instrumentation) as a method for gathering statistics. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.

## 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 good 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.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the following protocols:

- NetBIOS (from SiteScope installed on Windows platforms only)
- WMI (from SiteScope installed on Windows platforms only)
- SSH (from SiteScope installed on UNIX platforms only)

**Note:** When specifying a literal IPv6 address as the name for the monitored remote server when using the NetBIOS connection method, the IPv6 address must be customized by:

1. Replacing any colon (":") characters with a dash ("-") character.
2. Appending the text ".ipv6-literal.net" to the IP address.

For example, the IPv6 address: 2004:DB8:2a:1005:230:48ff:fe73:982d  
would be: 2004-DB8-2a-1005-230-48ff-fe73-982d.ipv6-literal.net

Alternatively, you can switch to the WMI connection method, and avoid having to make changes to the IPv6 address.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

# Tasks

## How to Configure the Service Monitor

### 1. Prerequisites

- Make sure you have the specific access permissions required for this monitor as specified in Permissions and Credentials.
- SiteScopes running on Windows platforms need 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. For SiteScopes installed on UNIX platforms, you only need to define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view.
- To avoid performance issues and monitor skips when running multiple perfex-based monitors against the same host, install the latest Microsoft **mrxsmb.sys** and **mrxsmb10.sys** or **mrxsmb20.sys** patch files on the SiteScope server. These files are available from <http://support.microsoft.com/kb/2847018/> and <http://support.microsoft.com/kb/2775511/> respectively.

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** The **Services Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Services Tool in the Using SiteScope Guide.

# UI Descriptions

## Service Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of 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> Remote servers that have been configured with the WMI method are also displayed here. For details, see Configure the WMI Service for Remote Monitoring in the Using SiteScope Guide.</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>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>



UI Element	Description
<b>Service</b>	<p>The service (or process in UNIX) that you want to monitor from the services list.</p> <p>To monitor a Windows 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></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Services are no longer automatically updated after opening the monitor's properties. Instead, click the <b>Reload Services</b> button to reload the selected services.</li> </ul>
<b>Reload Services</b>	Reloads the selected services.
<b>Other service</b>	<p>Name of the service you want to monitor (if it is not listed in the services list). Use a string or a regular expression.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• This field is available only when <b>Unknown</b> is selected in the <b>Service</b> box.</li> <li>• When using a regular expression, you must use lower case letters (for example, /hp.* /), or add "i" to the end of the expression (for example, /PATTERN/i).</li> </ul>
<b>Process name</b>	<p>(For Windows only) Name of the process 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. 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 Windows Task Manager.</li> <li>• This field is available only when (using Process name) is selected in the <b>Service</b> box.</li> </ul> <p><b>Example:</b> explorer.exe</p>
<b>Measure process memory use</b>	(For UNIX only) SiteScope reports the amount of virtual memory being used by a specific process.
<p><b>Note:</b> If you are editing the Service monitor settings from the Manage View of the Unified Console, the service options are categorized as follows:</p> <p><b>Service name from the list:</b> Select the name of the service that you want to monitor from the list.</p> <p><b>Service name Manually:</b> Type the name of the service you want to monitor if it is not listed in the services list.</p> <p><b>Process Name Manually:</b> Type the process name manually.</p>	

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Limitations

- 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.
- When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- Added the ability to reduce Service monitor runtime by adding the `_serviceMonitorOptByServiceName=true` property to the `<SiteScope root directory>\groups\master.config` file. This enables the monitor to retrieve data for the service selected for monitoring only, instead of retrieving all services from the remote machine, and then sorting for the selected service.
- Performance issues and monitor skips are encountered when running multiple perfex-based monitors against the same host. The server events and dump analysis reports issues with the **mrxsmb.sys** driver.  
**Solution:** Update the **mrxsmb.sys** file (via <http://support.microsoft.com/kb/2847018/>) and **mrxsmb10.sys/mrxsmb20.sys** files (via <http://support.microsoft.com/kb/2775511/>) by installing the Microsoft patches on the SiteScope server.

# Chapter 90: Siebel Application Server Monitor

The Siebel Application Server monitor uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel application servers.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of Siebel monitoring. For details, see Siebel Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Siebel Application Server monitor.

## Learn About

This section includes:

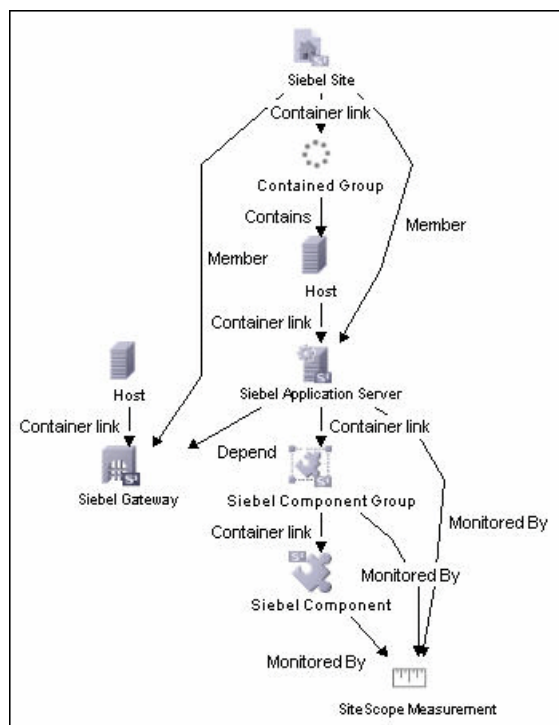
- ["Supported Platforms/Versions" below](#)
- ["Siebel Application Server Topology" below](#)
- ["License Consumption" on the next page](#)

### Supported Platforms/Versions

This 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, 8.0, 8.1, 8.2 - 8.2.2.4 application servers.

### Siebel Application Server Topology

The Siebel Application Server monitor can identify the topology of the Siebel Application Servers being monitored. The monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM as SiteScope Measurement Groups and SiteScope Measurement CIs.

**Note:** This direct integration between SiteScope and BSM is available only when the Application Management for Siebel license is installed.

For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

For information about the Siebel topology, see Siebel Views in the BSM User Guide in the BSM Help.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host Note: Monitor is not available when using Community edition.

## Tasks

### How to Configure the Siebel Application Server Monitor

#### 1. Prerequisites

- 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 **svrmgr** or **svrmgr.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 prefix in the Infrastructure Settings Preferences page; for example, change the **Prefix 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.`
- You can customize the command for connecting to the Siebel server in the **Siebel connect command** box in **Preferences > Infrastructure Preferences > Custom Settings** as follows:

```
_siebelConnectCommand=$PARAM_PATH$/srvmgr /g $PARAM_GATEWAY$ /e $PARAM_
ENTERPRISE$ /s $SERVER$ /u $PARAM_USERNAME$ /p $PARAM_PASSWORD$ /k %%%
```

where:

\$PARAM\_PATH\$ Full path to the Siebel Server Manager executable directory relative to the machine selected above.

\$PARAM\_GATEWAY\$ Siebel server name or address.

\$PARAM\_ENTERPRISE\$ Gateway server name or address.

\$SERVER\$ Enterprise server name or address.

\$PARAM\_USERNAME\$ Siebel user name.

\$PARAM\_PASSWORD\$ Siebel password.

All these values are taken from the monitor configuration.

## 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## 3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["Siebel Application Server Topology" on page 595](#).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

# UI Descriptions

## Siebel Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Siebel host name</b>	<p>Siebel host name 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>Windows Server Address</b> box for Windows remote servers or <b>Server Address</b> box for UNIX remote servers.</li><li>• <b>Reporting monitor data to an installation of Business Service Management.</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 a BSM report. The box is optional only if the <b>Script Server</b> box is already specified to be the target Siebel server.</li></ul>

UI Element	Description
<b>Application server</b>	Siebel server name or address.
<b>Gateway server</b>	Gateway server name or address.
<b>Enterprise server</b>	Enterprise server name or address.
<b>Credentials</b>	<p>Siebel Server Manager client requires a user name and password. 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 How to Configure Credential Preferences in the Using SiteScope Guide.</li> </ul>
<b>Script server</b>	<p>The remote Windows or UNIX machine where the Server Manager (srvmgr) 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>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>

UI Element	Description
<b>Script path</b>	<p>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>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p>
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Siebel Application Server Monitor" on page 595</a>.</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>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: <math>\text{time window} = (\text{current time} - \text{property value})</math>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.



## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<p><b>Siebel Server Statistics</b></p> <ul style="list-style-type: none"> <li>• Average Connect Time</li> <li>• Average Reply Size</li> <li>• Average Request Size</li> <li>• Average Requests Per Session</li> <li>• Average Response Time</li> <li>• Average Think Time</li> <li>• Avg SQL Execute Time</li> <li>• Avg SQL Fetch Time</li> <li>• Avg SQL Parse Time</li> <li>• CPU Time</li> <li>• Elapsed Time</li> <li>• Num of DBConn Retries</li> <li>• Num of DLRbk Retries</li> <li>• Num of Exhausted Retries</li> <li>• Number of Sleeps</li> <li>• Number of SQL Executes</li> <li>• Number of SQL Fetches</li> <li>• Number of SQL Parses</li> <li>• Object Manager Errors</li> <li>• Reply Messages</li> <li>• Request Messages</li> <li>• Sleep Time</li> <li>• SQL Execute Time</li> <li>• SQL Fetch Time</li> <li>• SQL Parse Time</li> <li>• Tests Attempted</li> <li>• Tests Failed</li> <li>• Tests Successful</li> <li>• Total Reply Size</li> <li>• Total Request Size</li> <li>• Total Response Time</li> <li>• Total Tasks</li> <li>• Total Think Time</li> </ul> <p><b>Component Statistics</b></p> <p>Call Center Object Manager</p> <ul style="list-style-type: none"> <li>• Average Connect Time</li> <li>• Average Reply Size</li> <li>• Average Request Size</li> <li>• Average Requests Per Session</li> </ul>	<ul style="list-style-type: none"> <li>• Average Response Time</li> <li>• Average Think Time</li> <li>• Number of SQL Parses</li> <li>• Number of Sleeps</li> <li>• Object Manager Errors</li> <li>• Reply Messages</li> <li>• Request Messages</li> <li>• Avg SQL Execute Time</li> <li>• Avg SQL Fetch Time</li> <li>• Avg SQL Parse Time</li> <li>• CPU Time</li> <li>• Elapsed Time</li> <li>• Number of SQL Executes</li> <li>• Number of SQL Fetches</li> <li>• SQL Execute Time</li> <li>• SQL Fetch Time</li> <li>• SQL Parse Time</li> <li>• Sleep Time</li> <li>• Total Reply Size</li> <li>• Total Request Size</li> <li>• Total Response Time</li> <li>• Total Tasks</li> <li>• Total Think Time</li> </ul> <p>File System Manager</p> <ul style="list-style-type: none"> <li>• Avg SQL Execute Time</li> <li>• Avg SQL Fetch Time</li> <li>• Avg SQL Parse Time</li> <li>• CPU Time</li> <li>• Elapsed Time</li> <li>• Num of DBConn Retries</li> <li>• Num of DLRbk Retries</li> <li>• Num of Exhausted Retries</li> <li>• Number of Sleeps</li> <li>• Number of SQL Executes</li> <li>• Number of SQL Fetches</li> <li>• Number of SQL Parses</li> <li>• Sleep Time</li> <li>• SQL Execute Time</li> <li>• SQL Fetch Time</li> <li>• SQL Parse Time</li> <li>• Total Tasks</li> </ul>	<p>Sales Object Manager</p> <ul style="list-style-type: none"> <li>• Average Connect Time</li> <li>• Average Reply Size</li> <li>• Average Request Size</li> <li>• Average Requests Per Session</li> <li>• Average Response Time</li> <li>• Average Think Time</li> <li>• Avg SQL Execute Time</li> <li>• Avg SQL Fetch Time</li> <li>• Avg SQL Parse Time</li> <li>• CPU Time</li> <li>• Elapsed Time</li> <li>• Number of SQL Executes</li> <li>• Number of SQL Fetches</li> <li>• Number of SQL Parses</li> <li>• Number of Sleeps</li> <li>• Object Manager Errors</li> <li>• Reply Messages</li> <li>• Request Messages</li> <li>• SQL Execute Time</li> <li>• SQL Fetch Time</li> <li>• SQL Parse Time</li> <li>• Sleep Time</li> <li>• Total Reply Size</li> <li>• Total Request Size</li> <li>• Total Response Time</li> <li>• Total Tasks</li> <li>• Total Think Time</li> </ul> <p>Server Manager</p> <ul style="list-style-type: none"> <li>• Avg SQL Execute Time</li> <li>• Avg SQL Fetch Time</li> <li>• Avg SQL Parse Time</li> <li>• CPU Time</li> <li>• Elapsed Time</li> <li>• Number of Sleeps</li> <li>• Number of SQL Executes</li> <li>• Number of SQL Fetches</li> <li>• Number of SQL Parses</li> <li>• Sleep Time</li> <li>• SQL Execute Time</li> <li>• SQL Fetch Time</li> <li>• SQL Parse Time</li> <li>• Total Tasks</li> </ul>
--	--	--

<p>Server Request Broker</p> <ul style="list-style-type: none"> <li>• Avg SQL Execute Time</li> <li>• Avg SQL Fetch Time</li> <li>• Avg SQL Parse Time</li> <li>• CPU Time</li> <li>• Elapsed Time</li> <li>• Num of DBConn Retries</li> <li>• Num of DLRbk Retries</li> <li>• Num of Exhausted Retries</li> <li>• Number of Sleeps</li> <li>• Number of SQL Executes</li> <li>• Number of SQL Fetches</li> <li>• Number of SQL Parses</li> <li>• Sleep Time</li> <li>• SQL Execute Time</li> <li>• SQL Fetch Time</li> <li>• SQL Parse Time</li> <li>• Total Tasks</li> </ul> <p>Server Request Processor</p> <ul style="list-style-type: none"> <li>• Avg SQL Execute Time</li> <li>• Avg SQL Fetch Time</li> <li>• Avg SQL Parse Time</li> <li>• CPU Time</li> <li>• Elapsed Time</li> <li>• Num of DBConn Retries</li> <li>• Num of DLRbk Retries</li> <li>• Num of Exhausted Retries</li> <li>• Number of Sleeps</li> <li>• Number of SQL Executes</li> <li>• Number of SQL Fetches</li> <li>• Number of SQL Parses</li> <li>• Sleep Time</li> <li>• SQL Execute Time</li> <li>• SQL Fetch Time</li> <li>• SQL Parse Time</li> <li>• Total Tasks</li> </ul> <p>Service Object Manager</p> <ul style="list-style-type: none"> <li>• Average Connect Time</li> <li>• Average Reply Size</li> <li>• Average Request Size</li> <li>• Average Requests Per Session</li> <li>• Average Response Time</li> <li>• Average Think Time</li> <li>• Avg SQL Execute Time</li> <li>• Avg SQL Fetch Time</li> <li>• Avg SQL Parse Time</li> <li>• CPU Time</li> <li>• Elapsed Time</li> <li>• Number of SQL Executes</li> <li>• Number of SQL Fetches</li> <li>• Number of SQL Parses</li> <li>• Number of Sleeps</li> </ul>	<ul style="list-style-type: none"> <li>• Object Manager Errors</li> <li>• Reply Messages</li> <li>• Request Messages</li> <li>• SQL Execute Time</li> <li>• SQL Fetch Time</li> <li>• SQL Parse Time</li> <li>• Sleep Time</li> <li>• Total Reply Size</li> <li>• Total Request Size</li> <li>• Total Response Time</li> <li>• Total Tasks</li> <li>• Total Think Time</li> </ul> <p>eService Object Manager</p> <ul style="list-style-type: none"> <li>• Average Connect Time</li> <li>• Average Reply Size</li> <li>• Average Request Size</li> <li>• Average Requests Per Session</li> <li>• Average Response Time</li> <li>• Average Think Time</li> <li>• Avg SQL Execute Time</li> <li>• Avg SQL Fetch Time</li> <li>• Avg SQL Parse Time</li> <li>• CPU Time</li> <li>• Elapsed Time</li> <li>• Number of Sleeps</li> <li>• Number of SQL Executes</li> <li>• Number of SQL Fetches</li> <li>• Number of SQL Parses</li> <li>• Object Manager Errors</li> <li>• Reply Messages</li> <li>• Request Messages</li> <li>• Sleep Time</li> <li>• SQL Execute Time</li> <li>• SQL Fetch Time</li> <li>• SQL Parse Time</li> <li>• Total Reply Size</li> <li>• Total Request Size</li> <li>• Total Response Time</li> <li>• Total Tasks</li> <li>• Total Think Time</li> </ul> <p>eTraining Object Manager</p> <ul style="list-style-type: none"> <li>• Average Connect Time</li> <li>• Average Reply Size</li> <li>• Average Request Size</li> <li>• Average Requests Per Session</li> <li>• Average Response Time</li> <li>• Average Think Time</li> <li>• Avg SQL Execute Time</li> <li>• Avg SQL Fetch Time</li> <li>• Avg SQL Parse Time</li> <li>• CPU Time</li> </ul>	<p><b>Component Objects</b></p> <p>Call Center Object Manager</p> <ul style="list-style-type: none"> <li>• CP_ACTV_MTS Component</li> <li>• CP_DISP_RUN_STATE</li> <li>• CP_MAX_MTS • CP_MAX_TASK</li> </ul> <p>File System Manager</p> <ul style="list-style-type: none"> <li>• CP_ACTV_MTS Component</li> <li>• CP_DISP_RUN_STATE</li> <li>• CP_MAX_MTS</li> <li>• CP_MAX_TASK</li> </ul> <p>Sales Object Manager</p> <ul style="list-style-type: none"> <li>• CP_ACTV_MTS Component</li> <li>• CP_DISP_RUN_STATE</li> <li>• CP_MAX_MTS</li> <li>• CP_MAX_TASK Server Manager</li> <li>• CP_ACTV_MTS Component</li> <li>• CP_DISP_RUN_STATE</li> <li>• CP_MAX_MTS</li> <li>• CP_MAX_TASK Server Request Broker</li> <li>• CP_ACTV_MTS Component</li> <li>• CP_DISP_RUN_STATE</li> <li>• CP_MAX_MTS • CP_MAX_TASK</li> </ul> <p>Server Request Processor</p> <ul style="list-style-type: none"> <li>• CP_ACTV_MTS Component</li> <li>• CP_DISP_RUN_STATE</li> <li>• CP_MAX_MTS</li> <li>• CP_MAX_TASK</li> </ul> <p>Service Object Manager</p> <ul style="list-style-type: none"> <li>• CP_ACTV_MTS Component</li> <li>• CP_DISP_RUN_STATE</li> <li>• CP_MAX_MTS</li> <li>• CP_MAX_TASK</li> </ul> <p>eService Object Manager</p> <ul style="list-style-type: none"> <li>• CP_ACTV_MTS Component</li> <li>• CP_DISP_RUN_STATE</li> <li>• CP_MAX_MTS</li> <li>• CP_MAX_TASK</li> </ul> <p>eTraining Object Manager</p> <ul style="list-style-type: none"> <li>• CP_MAX_TASK</li> <li>• CP_ACTV_MTS Component</li> <li>• CP_MAX_MTS</li> <li>• CP_DISP_RUN_STATE</li> </ul>
---	--	--

## Tips/Troubleshooting

### General Notes/Limitations

- When configuring this monitor in template mode, the **Browse Servers**, **Add Remote Server**, and **Add Credentials** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

### Troubleshooting

To fix Siebel Application Server monitor skips in high load environments, add the **\_siebelDataCacheTimeout** property to the **<SiteScope root directory>\groups\master.config** file, and enter a timeout value in seconds.

# Chapter 91: Siebel Log File Monitor

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 receive warnings before issues escalate into more serious problems.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of Siebel monitoring. For details, see Siebel Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Siebel Log File monitor.

## Learn About

This section includes:

- ["Siebel Log File Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Monitor Counters" below](#)
- ["License Consumption" on the next page](#)

### Siebel Log File Monitor Overview

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.

Each time that SiteScope runs this monitor, it starts from the point in the file where it stopped reading last time it ran. This ensures 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.

### Supported Platforms/Versions

This monitor supports monitoring remote servers running on Siebel Application Server 7.03, 7.04, 7.5.3, 7.7, 8.0, 8.1, 8.2 - 8.2.2.4.

### Monitor Counters

The following counter can be configured for this monitor: matchCount. This monitors the number of events matched by regular expression. For details on regular expressions, see Regular Expressions.

## License Consumption

Point-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitored host  Note: Monitor is not available when using Community edition.

## Tasks

### How to Configure the Siebel Log File Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### Siebel Log File Monitor Settings

User interface elements are described below:

UI 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>

UI Element	Description
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</p>
<b>Add Remote Server</b>	<p>Opens the Add Remote Server dialog box, enabling you to 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 in the Using SiteScope Guide.</p> <p>For details on the UNIX Remote Servers user interface, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Log file directory</b>	<p>Path to the log directory you want to monitor.</p> <p>To monitor log files on a remote Windows 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 Windows server, you must select the java library and ssh1 options for that remote.</p>
<b>File name (regular expr.)</b>	<p>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>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>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>

UI Element	Description
<b>Log-entry content match</b>	(Optional) 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.  You use this option to find only those log entries with the selected severity an event type that meet this additional match criterion.
<b>Search from start</b>	Always checks 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).  <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.  <b>Default value:</b> Not selected

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

The Siebel Log File Monitor watches for log file entries added to a group of log files by looking for entries containing a specific event type or subtype. Use this page to add the monitor or edit the monitor's properties.

- matchCount – number of events matched by a regular expression

# Tips/Troubleshooting

## General Notes/Limitations

When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

# Chapter 92: Siebel Web Server Monitor

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.

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of Siebel monitoring. For details, see Siebel Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Siebel Web Server monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["Siebel Web Server Topology" below](#)
- ["License Consumption" on the next page](#)

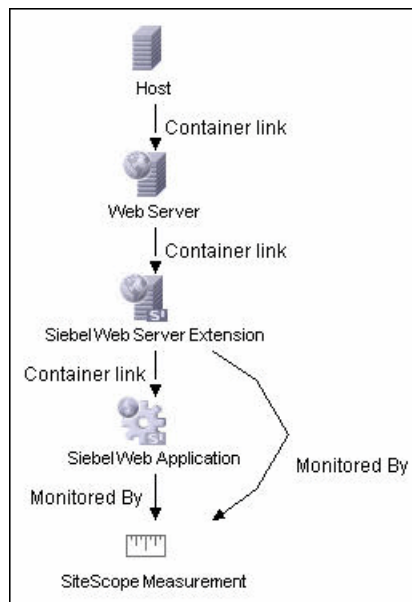
### Supported Platforms/Versions

This monitor supports monitoring remote servers running on Siebel Application Server 7.03, 7.04, 7.5.3, 7.7, 8.0, 8.1, 8.2 - 8.2.2.4.

### Siebel Web Server Topology

The Siebel Web Server monitor can identify the topology of the Siebel Web Server being monitored. The monitor creates the following topology in BSM's RTSM.





The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM as SiteScope Measurement Groups and SiteScope Measurement CIs.

**Note:** This direct integration between SiteScope and BSM is available only when the Application Management for Siebel license is installed.

For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

For information about the Siebel topology, see Siebel Views in the BSM User Guide in the BSM Help.

## License Consumption

Point-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitor
	Note: Monitor is not available when using Community edition.

# Tasks

## How to Configure the Siebel Web Server Monitor

### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- This monitor requires the Siebel solution templates to enable it in the SiteScope interface (requires Trial, Premium, Ultimate, or System Collector edition). For information about using templates to deploy monitors, see SiteScope Templates in the Using SiteScope Guide.

To use the monitor, you must have an Operating System Instance (OSi) license with sufficient available capacity.

- 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. Refer to the Siebel documentation for more information.

2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["Siebel Web Server Topology" on page 608](#).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

## UI Descriptions

### Siebel Web Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Basic Settings</b>	
<b>Application URL</b>	URL of the Web plug-in server stats page for the application you want to monitor. <b>Example:</b> <code>http://siebelsrv/service/_stats.swe</code>  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.
<b>Counters</b>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on page 612</a> .  <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.
<b>Connection Settings</b> (These settings are optional, unless the server requires authentication)	

UI Element	Description
<b>Authorization user name</b>	User name to access the Web server stats page.
<b>Authorization password</b>	Password for accessing the Web server stats page.
<b>HTTP proxy</b>	Proxy server and port to use if you are using a proxy to access the Siebel server. <b>Example:</b> proxy.SiteScope.com:8080
<b>Proxy server user name</b>	Proxy user name if the proxy server requires authorization.
<b>Proxy server password</b>	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>	SiteScope submits HTML form-based authentication when accessing the Siebel Web server plug-in.
<b>Authorization form name</b>	Authentication form identifier within the Web page when using HTML Form-based Authentication. 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.
<b>Authorization user name form field</b>	User name that should be submitted to the access control system when using HTML Form-based Authentication. 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>	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.

UI Element	Description
<b>Authorization form button</b>	<p>Identifier of the Submit button on the authentication form when using HTML Form-based Authentication.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<p><u>System Statistics</u></p> <p>Anonymous sessions requested from the pool</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p>Open Session Time</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p>Anon Session Available</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p>Close Session Time</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p>Request Time</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p>Anon Session Removed</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p>Response Time</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> </ul>	<ul style="list-style-type: none"> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p>Anonymous sessions returns to the pool</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p><u>Applications</u></p> <p>/sales/Session Lifespan</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p>/sales/</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p>/callcenter/</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul> <p>/callcenter/Session Lifespan</p> <ul style="list-style-type: none"> <li>• Frequency mean</li> <li>• Frequency stddev</li> <li>• General Stats count</li> <li>• General Stats mean</li> <li>• General Stats stddev</li> <li>• Value</li> </ul>
--	--

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 93: SNMP Monitor

This monitor enables you to monitor devices that communicate with the SNMP protocol, such as firewalls, routers, and UPS systems.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SNMP monitor.

## Learn About

This section includes:

- ["SNMP Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" on the next page](#)

## SNMP Monitor Overview

Many network devices support the SNMP protocol as a way of monitoring them. 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.

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 Object ID that maps to that value. The Object ID's may be available in the product documentation or in the form of a MIB file. 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.

## Supported Platforms/Versions

- This monitor supports monitoring agents of SNMP versions 1.0, 2.0, and 3.0 MD5 and SHA.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license for 10 monitors

# Tasks

## How to Configure the SNMP Monitor

### 1. Prerequisites

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. For more details on user permissions and credentials required for this monitor, see [Permissions and Credentials](#).
- 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 [HPE Software Self-solve Knowledge Base](https://softwaresupport.hp.com/group/softwaresupport/search-result) (<https://softwaresupport.hp.com/group/softwaresupport/search-result>). To enter the knowledge base, you must log on with your HPE Passport ID.

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the [UI Descriptions](#) section below.

**Tip:** The **SNMP Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see [SNMP Tool](#).



## UI Descriptions

### SNMP Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Basic SNMP Settings</b>	
<b>Host name</b>	Host name or IP address of the SNMP device that you want to monitor (for example, demo.thiscompany.com).
<b>Port</b>	Port to use when requesting data from the SNMP agent. <b>Default value:</b> 161

UI Element	Description
<b>Object ID</b>	<p>Select the Object ID setting:</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.) Enter the index of the SNMP object. Values for an OID come as either scalar or indexed (array or table) values. <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. The index value for Commonly used values is set to <code>ifSpecific.ifInOctets</code>.</li> </ul> <p><b>Default value:</b> 0</p> </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. <b>Example:</b> 1.3.6.1.2.1.4.3</li> </ul> <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 supports SNMP versions 1.0, 2.0, and 3.0.</p> <p>If you receive the error message error - noSuchName, 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 Tools &gt; MIB Browser 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 browse 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>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>

UI Element	Description
<b>Secondary object ID</b>	<p>Secondary object ID and Secondary match content are used for creating a new Object ID and for getting data for it. The SNMP monitor gets data using the main Object ID, and the data that is matched by the Secondary match content {index corresponding to the group} is used in the Secondary object ID.</p> <p><b>Example:</b> Secondary match content matches the first digit and can be used in the Secondary object ID using the next construction 1.3.6.5.{0}, or it can match the full Object ID and the Secondary object ID can be set using the next construction {0}.</p> <p>(To enable secondary object changes, you must add the property <code>_enableSecondSNMP=true</code> to the <code>master.config</code> file.)</p>
<b>Secondary match content</b>	<p>Sets up a secondary SNMP index. Match this item against the main SNMP value using a string, regular expression (see Regular Expressions Overview), or XML names (see Monitoring XML Documents Overview in the Using SiteScope Guide).</p> <p><b>Example:</b> <code>/(\d)/</code> gets the first digit and uses it in the secondary index.</p>
<b>SNMP Connection Settings</b>	
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, that SiteScope should wait for an SNMP request.</p> <p><b>Default value:</b> 5 seconds</p>
<b>Number of retries</b>	<p>Number of SNMP request retries before SiteScope considers the monitor to have failed.</p> <p><b>Default value:</b> 1</p>
<b>Community</b>	<p>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>
<b>SNMP version</b>	<p>SNMP version used by the SNMP host you want to monitor. SiteScope supports SNMP version 1, version 2, and version 3.</p> <p><b>Default value:</b> V1</p>
<b>Authentication algorithm</b>	<p>Authentication algorithm used for SNMP V3. You can select MD5, SHA, or None.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>User name</b>	<p>User name to be used for authentication if you are using SNMP version 3.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>

UI Element	Description
<b>Password</b>	Password to be used for authentication if you are using SNMP version 3. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Privacy algorithm</b>	The privacy algorithm used for authentication for SNMP version 3 (DES, 128-Bit AES, 192-Bit AES, 256-Bit AES). <b>Default value:</b> DES <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Privacy password</b>	The privacy password used for authentication for SNMP version 3. Leave blank if you do not want privacy. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Context name</b>	The context name of SNMP version 3. <b>Note:</b> This field is available only if SNMP V3 is selected.
<b>Context engine ID</b>	The context engine ID of SNMP version 3. <b>Note:</b> This field is available only if SNMP V3 is selected.
<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 to match against an SNMP value, using a string or a regular expression or XML names.
<b>Open Tool</b>	Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.
<b>Units</b>	Optional units string to append when displaying the value of this counter.
<b>Measurement label</b>	Optional text string to describe the measurement being made by the monitor.
<b>Measure as delta</b>	Reports the measurement as the difference between the current value and the previous value.
<b>Measure as rate per second</b>	Divides the measurement by the number of seconds since the last measurement.

UI Element	Description
<b>Percentage base</b>	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.  <b>Default value:</b> No percentage base
<b>Measure base as delta</b>	Calculates 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>	Maximum value for the Object ID. The maximum is calculated to create the gauge display (Optional).

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

Any value available via SNMP MIBs for the device.

- content match
- status
- value

# Chapter 94: SNMP by MIB Monitor

The SNMP by MIB monitor enables you to monitor objects on any SNMP agent.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SNMP by MIB monitor.

## Learn About

This section includes:

- ["SNMP by MIB Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" on the next page](#)

### 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 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 a 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.

The error and warning thresholds for the monitor can be set on one or more different objects.

### Supported Platforms/Versions

- This monitor supports monitoring agents of SNMP versions 1, 2, and 3 MD5.
- This monitor supports monitoring remote servers running on the following Windows operating systems: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012.

### IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Point-based Usage	Capacity-based Usage
One point per metric	One OSi license for 10 monitors

# Tasks

## How to Configure the SNMP by MIB Monitor

### 1. Prerequisites

Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.

### 2. 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.

- 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.
- 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.
- 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 627](#).

### 3. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** The **SNMP Browser Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Browser Tool in the Using SiteScope Guide.

# UI Descriptions

## SNMP by MIB Monitor Settings

User interface elements are described below:

UI Element	Description
<b>SNMP Settings</b>	
<b>Server</b>	Name of the server you want to monitor.
<b>Port</b>	Port to use when requesting data from the SNMP agent. <b>Default value:</b> 161
<b>MIB File</b>	<p>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 a 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 <b>&lt;SiteScope root directory&gt;\templates.mib</b> directory and restart SiteScope.</p> <b>Default value:</b> All MIBs
<b>Counter calculation mode</b>	<p>Performs 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> <b>Default value:</b> Do not calculate



UI Element	Description
<b>Starting OID</b>	<p>Use 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>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> <p><b>Note:</b> This field is available in template mode only.</p>
<b>SNMP Connection Settings</b>	
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, that SiteScope should wait for an SNMP request.</p> <p><b>Default value:</b> 5 seconds</p>
<b>Number of retries</b>	<p>Number of SNMP request retries before SiteScope considers the monitor to have failed.</p> <p><b>Default value:</b> 1</p>
<b>Community</b>	<p>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>
<b>SNMP version</b>	<p>Version of SNMP to use when connecting. SiteScope supports SNMP version 1, version 2, and version 3. Selecting V3 enables you to enter version 3 settings in the fields below.</p> <p><b>Default value:</b> V1</p>
<b>Authentication algorithm</b>	<p>Authentication algorithm used for SNMP V3. You can select MD5, SHA, or None.</p> <p><b>Default value:</b> MD5</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>User name</b>	<p>User name for version 3 connections.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>Password</b>	<p>Authentication password to use for version 3 connections.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>

UI Element	Description
<b>Privacy algorithm</b>	<p>The privacy protocol used for authentication for SNMP version 3 (DES, 128-Bit AES, 192-Bit AES, 256-Bit AES). Leave blank if you do not want privacy.</p> <p><b>Default value:</b> DES</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>Privacy password</b>	<p>Privacy password for version 3 connections. Leave blank if you do not want privacy.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>Context name</b>	<p>Context Name to use for this connection. This is applicable for SNMP V3 only.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>Context engine ID</b>	<p>Hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.</p> <p><b>Note:</b> This field is available only if SNMP V3 is selected.</p>
<b>SNMP Counters</b>	
<b>Counters</b>	<p>Displays 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>Opens the Select Counters Form, enabling you to select the counters you want to monitor.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>At first, only the MIB tree is loaded. Choose the required MIB node you want to monitor, and right-click it to load counters from the remote device.</li> <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> </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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

Any value available via SNMP MIBs for the device.

# Tips/Troubleshooting

## General Notes/Tips

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

## 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 step 1 of ["How to Configure the SNMP by MIB Monitor" on page 623](#) to verify that the new MIB files compiled correctly.

# Chapter 95: SNMP Trap 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SNMP Trap monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" below](#)
- ["License Consumption" below](#)

## Supported Platforms/Versions

The monitor supports monitoring traps of SNMP versions 1, 2, and 3.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## License Consumption

Point-based Usage	Capacity-based Usage
One point per monitor	One OSi license for 15 monitors

## Tasks

### How to Configure the SNMP Trap Monitor

#### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- You must configure the network devices to send SNMP Traps to SiteScope. 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.

## 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** The **SNMP Trap Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Trap Tool in the Using SiteScope Guide.

# UI Descriptions

## SNMP Trap Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Content match</b>	<p>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 <b>&lt;SiteScope root directory&gt;\logs\SNMPTrap.log</b> 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>

UI Element	Description
Match value labels	<p>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>
Run alerts	<p>Method for running alerts:</p> <ul style="list-style-type: none"><li>• <b>For each SNMP Trap matched.</b> 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>• <b>Once, after all SNMP Traps have been checked.</b> 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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Limitations

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.

# Chapter 96: Solaris Zones Monitor

The Solaris Zones monitor enables you to monitor the physical host, its zones, and their resource pools on Solaris servers.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Solaris Zones monitor.

## Learn About

This section includes:

- ["Solaris Zones Topology" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Virtualization Support" below](#)
- ["Solaris Zones Topology" below](#)
- ["License Consumption" on the next page](#)

## 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 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 [How to Configure SiteScope to Monitor a Remote UNIX Server](#) in the Using SiteScope Guide.

For details on how to analyze Solaris zones monitor results, see ["How to Analyze Solaris Zones Monitor Results – Use-Case Scenario" on page 633](#).

## Supported Platforms/Versions

This monitor supports monitoring machines that are running on the following Solaris operating systems: Solaris 10 update 7 (5/09) - Solaris 10 update 11 (01/13), Solaris 11.2.

## Virtualization Support

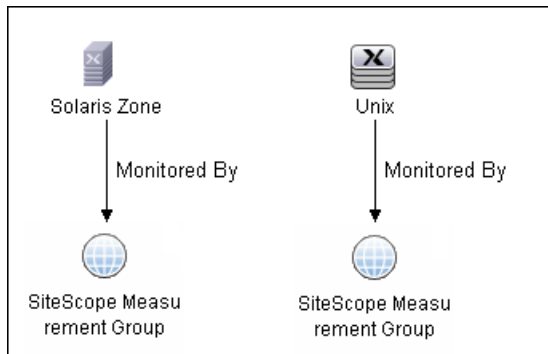
A Solaris zone is a virtualized operating system environment created within a single instance of the Solaris Operating System. It provides the required isolation and security to run multiple applications of the same operating system on the same server.

**Note:** Branded zones that are not of Solaris type are not supported.

## Solaris Zones Topology

The Solaris Zones monitor can identify the topology of the Solaris system being monitored. If **Report monitor**

**and related CI topology** is selected in **HP Integration Settings** (the default setting), the monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select. The monitors are represented in the RTSM 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 BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
<p>One point for each monitored zone (global or non-global) or physical server.</p> <p>Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.</p>	<p>One OSi per monitored server property and One OSi per monitored zone</p>

## Tasks

This section includes:

- ["How to Configure the Solaris Zones Monitor" below](#)
- ["How to Analyze Solaris Zones Monitor Results – Use-Case Scenario" on the next page](#)

### How to Configure the Solaris Zones Monitor

1. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

2. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["Solaris Zones Topology" on the previous page](#).



For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

## How to Analyze Solaris Zones Monitor Results – Use-Case Scenario

This use-case scenario describes how the Solaris Zones monitor can be used to diagnose problems on the physical host, and in the zone and resource pool level.

- **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.

- **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.

- **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.

- **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.

# UI Descriptions

## Solaris Zones Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of 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>Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.</p>
<b>Counters</b>	<p>Displays 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> <p><b>Note:</b> When configuring this monitor in template mode, you can use regular expressions to define counters.</p>
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

### Per- Zone counters:

- %usageOfMachineCpu – Usage (in %) of total cpu on the machine
- %usageOfPoolCpu – Usage (in %) of total cpu in the zone pool

### Non-Global Zones:

- %usr – Portion of time spent in user mode by the processors in this zone's pool (or in the default pool if no pool is used)
- %sys – Portion of time spent in system mode by the processors in this zone's pool (or in the default pool if no pool is used)
- %idle – Portion of time spent idle (but not waiting for block IO) by the processors in this zone's pool (or in the default pool if no pool is used)
- %wio – Portion of time spent idle with some process waiting for block IO by the processors in this zone's pool (or in the default pool if no pool is used)
- mbRss – Memory resident set size in MB
- mbSize – Total of virtual memory size in MB
- %memory – Percentage of memory used
- inputPackets – Num of input packets on this logical interface that were received successfully
- outputPackets – Num of output packets on this logical interface that were transmitted successfully
- kbUsed – KB used on this file system
- kbAvail – KB available on this file system
- %capacity – Percentage of used space out of total capacity on this file system

### Physical machine counters:

- %usr – Portion of time spent in user mode by all the processors on this system
- %sys – Portion of time spent in system mode by all the processors on this system
- %idle – Portion of time spent idle (but not waiting for block IO) by all the processors on this system
- %wio – Portion of time spent idle with some process waiting for block IO by all the processors on this system
- inputPackets – Num of input packets on this physical interface that were received successfully
- outputPackets – Num of output packets on this physical interface that were transmitted successfully
- errInputPackets – Num of input packets with errors on this physical interface
- errOutputPackets – Num of failed attempts made to transmit a package on this physical interface
- collis – Num of failed attempts to transmit a package on this physical interface that have been prevented by another machine trying to transmit at the same time
- %networkErrs – Percentage of packets in errs out of all packets on this physical interface
- %collisofOpkts – Percentage of collisions out of packets transmitted successfully on this physical interface
- %errsOfpkts – Percentage of error input packets out of packets received correctly on this physical interface
- readsPerSecond – Reads per second on this device
- writesPerSecond – Writes per second on this device
- kbReadPerSecond – KB read per second on this device
- kbWrittenPerSecond – KB written per second on this device
- kbFreeMemory – Free memory in KB
- kbAvailableVirtualMemory – Sum (in KB) of free RAM and free disk swap space not reserved by processes or the kernel
- kbPageInPerSecond – KB Paged-in per second
- kbPageOutPerSecond – KB Paged-out per second

### Pool counters:

- %used – Percentage of pool resource in use

# Tips/Troubleshooting

## General Notes/Tips

- The monitor collects measurements for the zones that are in **Running** state only.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

## 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.
- The Solaris Zone monitor uses the SAR command to monitor CPU usage of physical and non-global zones of Solaris machines. To monitor non-global zones on a Solaris 11.2 operating system, the SAR tool should be configured and enabled in all zones.
- 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 **zonectfg** 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 **zonectfg**), 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 BSM. 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.

# Chapter 97: SunONE Web Server Monitor

This monitor enables you to monitor the availability of SunONE or iPlanet servers using the stats-xml performance metrics file (iwsstats.xml or nesstats.xml) facility.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the SunONE Web Server monitor.

## Learn About

### SunONE Web Server Monitor Overview

Use the SunONE Web Server monitor to monitor performance metrics reported in the stats-xml file of SunONE or iPlanet 6.x servers. 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.

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. Error and warning thresholds for the monitor can be set on one or more SunONE server performance statistics or HTTP response codes.

### Supported Platforms/Versions

This monitor supports monitoring SunONE or iPlanet 6.x or 7.0 servers.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitor

## Tasks

### How to Configure the SunONE Web Server Monitor

#### 1. Prerequisites

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.

2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### SunONE Web Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>Stats-XML URL</b>	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>	User name of the SunONE server you want to monitor.
<b>Authorization password</b>	Password of the SunONE server you want to monitor.
<b>HTTP proxy</b>	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the server.
<b>Proxy server user name</b>	Proxy server user name if the proxy server requires a name and password to access the server.  <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	Proxy server password if the proxy server requires a name and password to access the server.
<b>Timeout (seconds)</b>	Amount of time, in seconds, to 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>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. 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.
<b>Counter Settings</b>	
<b>Counters</b>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.

UI Element	Description
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.



## Monitor Counters

Below is the list of counters that can be configured for this monitor:

versionMajor versionMinor enabled • server • id • versionServer • timeStarted • secondsRunning • ticksPerSecond • maxProcs • maxThreads • maxVirtualServers • flagProfilingEnabled • flagVirtualServerOverflow • connection-queue • id thread-pool • id • name process • pid • mode • timeStarted • countConfigurations • connection-queue-bucket connection-queue countTotalConnections countQueued peakQueued maxQueued countOverflows countTotalQueued ticksTotalQueued • thread-pool-bucket thread-pool countThreadsIdle countThreads maxThreads countQueued peakQueued maxQueued	• dns-bucket flagCacheEnabled countCacheEntries maxCacheEntries countCacheHits countCacheMisses flagAsyncEnabled countAsyncNameLookups countAsyncAddrLookups countAsyncLookupsInProgress • keepalive-bucket countConnections maxConnections countHits countFlushes countRefusals countTimeouts secondsTimeout • cache-bucket flagEnabled secondsMaxAge countEntries maxEntries countOpenEntries maxOpenEntries sizeHeapCache maxHeapCacheSize sizeMmapCache maxMmapCacheSize countHits countMisses countInfoHits countInfoMisses countContentHits countContentMisses virtual-server id mode hosts interfaces	request-bucket • method • uri • countRequests • countBytesReceived • countBytesTransmitted • rateBytesTransmitted • maxByteTransmissionRate • countOpenConnections • maxOpenConnections • count2xx • count3xx • count4xx • count5xx • countOther • count200 • count302 • count304 • count400 • count401 • count403 • count404 • count503 Derived Counters process/% File info cache hits process/% Cache heap utilization process/% Cache memory utilization process/% File content cache hits process/% DNS cache utilization process/% Idle threads process/% File cache hits process/% DNS cache misses process/% Cache table utilization process/% DNS cache hits
---	---	--

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 98: Sybase Monitor (Deprecated)

**Note:** The Sybase monitor was deprecated. If this monitor was configured in a previous version of SiteScope, it is still displayed in SiteScope after performing an upgrade (but will not work). This monitor is supported in SiteScope 11.24 and earlier versions.

The Sybase monitor enables you to monitor the availability and performance statistics of a Sybase 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 Sybase server in your environment. The error and warning thresholds for the monitor can be set on one or more Sybase server performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Sybase monitor.

## Learn About

### Supported Platforms/Versions

- This monitor supports monitoring the server performance data for Sybase 11.0, 11.5, 11.92, 12.x, and 15.5 database servers.
- This monitor is supported in SiteScopes that are running on Windows versions only.
- This monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.

## Tasks

### How to Configure the Sybase Monitor

#### 1. Prerequisites

- Before you can use the Sybase monitor, you have to configure the Sybase server environment. The Sybase monitor connects to the Sybase Adaptive Server Enterprise (ASE) server by using the ASE Monitor Server and retrieves metrics from the server using Sybase-provided libraries. When connecting to the monitored server, you connect to the ASE Monitor Server, not the Sybase server. The ASE Monitor Server is an application that runs on the same machine as Sybase server and retrieves performance information from the Sybase server. The ASE 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 ASE Monitor Server for that server would be `back-endddb_ms`.
- Make sure that your ASE Monitor Server has all EBF updates and works correctly. To download the updates, log on to the Sybase web site, and in the **Support** menu, select **EBFs/Update > EBFs/Maintenance > Adaptive Server Enterprise**. (A Sybase account is required to access this

page.)

- Make sure your version of Sybase Central supports getting counters from an ASE Monitor Server; Sybase stopped support for ASE Monitor Server on 9/30/2012 (<http://www.sybase.com/detail?id=1089011>).
- You also have to install the Sybase Central client on the machine where SiteScope is running to connect to the ASE 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 ASE Monitor Server.

## 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## Sybase Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	Name of the server you want to monitor. Usually it is the name of the server followed by <b>_MS</b> .
<b>User name</b>	User name to access the Sybase database.
<b>Password</b>	Password of the user name to access the Sybase database.
<b>Counters</b>	Displays 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>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see " <a href="#">Monitor Counters</a> " on the next page.  <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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<p><b>Application</b> No Counters Currently Available</p> <p><b>Cache</b></p> <ul style="list-style-type: none"> <li>• % Hits</li> <li>• Pages from disk(read)</li> <li>• Pages from disk(read)/sec</li> <li>• Pages write</li> <li>• Pages write/sec</li> <li>• Pages(Read)</li> <li>• Pages(Read)/sec</li> </ul> <p><b>Disk</b></p> <ul style="list-style-type: none"> <li>• Master</li> <li>• Reads</li> <li>• Reads/sec</li> <li>• Writes</li> <li>• Writes/sec</li> <li>• Waits</li> <li>• Waits/sec</li> <li>• Grants</li> <li>• Grants/sec</li> </ul> <p><b>Engine</b></p> <ul style="list-style-type: none"> <li>• CPU time</li> <li>• Logical pages(Read)</li> <li>• Logical pages(Read)/sec</li> <li>• Pages from disk(Read)</li> <li>• Pages from disk(Read)/sec</li> <li>• Pages stored</li> <li>• Pages stored/sec</li> <li>• Server is busy(%)</li> </ul>	<p><b>Lock</b></p> <ul style="list-style-type: none"> <li>• % Requests</li> <li>• Granted after wait</li> <li>• Granted after wait/sec</li> <li>• Granted immediately</li> <li>• Granted immediately/sec</li> <li>• Locks count</li> <li>• Locks count/sec</li> <li>• Not granted</li> <li>• Not granted/sec</li> <li>• Wait time(avg)</li> </ul> <p><b>Memory Manager</b></p> <ul style="list-style-type: none"> <li>• Cache size</li> </ul> <p><b>Network</b></p> <ul style="list-style-type: none"> <li>• Average packet size(Read)</li> <li>• Average packet size(Send)</li> <li>• Network bytes(Read)</li> <li>• Network bytes(Read)/sec</li> <li>• Network bytes(Send)</li> <li>• Network bytes(Send)/sec</li> <li>• Network Packets(Read)</li> <li>• Network Packets(Read)/sec</li> <li>• Network Packets(Send)</li> <li>• Network Packets(Send)/sec</li> </ul> <p><b>Process</b></p> <ul style="list-style-type: none"> <li>• % Cache Hit</li> <li>• % Processor Time (process)</li> <li>• Locks/sec</li> <li>• Pages (write)</li> </ul>	<p><b>SqlSrvr</b></p> <ul style="list-style-type: none"> <li>• % Processor Time(server)</li> <li>• Deadlocks</li> <li>• Locks/sec</li> <li>• Transactions</li> </ul> <p><b>Stored procedures</b></p> <ul style="list-style-type: none"> <li>• Avg. Duration (sampling period)</li> <li>• Avg. Duration (session)</li> <li>• Executed (sampling period)</li> <li>• Executed (session)</li> </ul> <p><b>Transaction</b></p> <ul style="list-style-type: none"> <li>• Inserts</li> <li>• Inserts/sec</li> <li>• Rows(deleted)</li> <li>• Rows(deleted)/sec</li> <li>• Transactions</li> <li>• Transactions/sec</li> <li>• Updates</li> <li>• Updates in place</li> <li>• Updates in place/sec</li> <li>• Updates/sec</li> </ul>
---	--	--

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 99: Syslog Monitor

Use this monitor to check for specific entries added to a log file on a UNIX or Linux environment by looking for entries containing a text phrase or a regular expression.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Syslog monitor.

## Learn About

This section includes:

- ["Syslog Monitor Overview" below](#)
- ["Support for IPv6" below](#)
- ["License Consumption" below](#)

### Syslog Monitor Overview

The Syslog monitor is used for monitoring Syslog processes and messages from UNIX and Linux remote servers. It watches for specific entries containing a text phrase or a regular expression in log files that were determined in the **syslog.conf (rsyslog.conf)** file. All UNIX and Linux systems supported by SiteScope are POSIX-compliant (partially or fully), and all of them use syslog for logging various system events.

You can use the monitor 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 648](#).

### Support for IPv6

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, the SSH protocol is supported.

For details on using IPv6, see Support for IP Version 6 in Using SiteScope.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitor

# Tasks

This section includes:

- ["How to Configure the Syslog Monitor" below](#)
- ["Customizing Syslog Content Matches and Monitor Alerts" below](#)

## How to Configure the Syslog Monitor

### 1. Prerequisites

The following configuration requirements must be performed or verified before the Syslog monitor can be used:

- The remote server should be created with credentials that grant read access on the monitored file. For more details on user permissions and credentials required for this monitor, see Permissions and Credentials.
- The **rsyslog.conf** file on the remote machine must be backward compatible with the **syslog.conf** file.
- The **syslog.conf** (**rsyslog.conf**) file 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 path to **syslog.conf** (**rsyslog.conf**) can be determine for each operating system in the **<SiteScope root directory>\templates.os** folder in the syslog section.
- SiteScope is unable to execute a command with more than 80 characters on a remote UNIX server via a Telnet connection (the "unable to read log file" message is displayed in the monitor summary). To avoid this issue, increase the COLUMNS variable in the UNIX shell script that customized the shell environment (for bash this is `.bashrc`).

### 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## Customizing Syslog Content Matches and Monitor Alerts

You can create a Syslog monitor that triggers customized alerts for content matches according to the threshold status of the monitor.

### To configure the Syslog monitor with custom matches and alerts:

1. In the Syslog Monitor Settings, configure the following settings:
  - **Run alerts:** Select the **For each log entry matched** option.
  - **Process match** and **Message 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)/`. The test string from both of these fields is combined in one regular expression, which is displayed in the **Regular expression preview** box. You can determine how the strings are combined in the **System log match regular expression** box in **Preferences > Infrastructure Preferences > Custom Settings**.
2. Configure error, warning, and good alerts for the Syslog 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 [How to Configure an Alert in the Using SiteScope Guide](#).

## UI Descriptions

### Syslog Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>Server</b>	<p>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>
<b>Log file path</b>	<p>Path to the log file from which you want to extract data. Lists log files from <b>syslog.conf</b> with information of messages stored in that log.</p> <p><b>Examples:</b></p> <ul style="list-style-type: none"><li>• /var/log/messages (*.info;mail.none;authpriv.none;cron.none )</li><li>• /var/log/secure (authpriv.*)</li><li>• /var/log/maillog (mail.*)</li></ul>
<b>Add Remote Server</b>	<p>Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see <a href="#">New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide</a>.</p>

UI Element	Description
<b>Run alerts</b>	<p>Method for running alerts for this monitor.</p> <ul style="list-style-type: none"> <li>• <b>For each log entry matched.</b> The monitor triggers alerts according to thresholds applied to each matching entry found. Since status can change according to thresholds for each matched entry, each alert action could be triggered many times within a monitor run. Syslog can write repetitive entries as "last message repeated N times" instead of writing identical messages to the log file (this does not work for <b>Server-side processing</b>).</li> </ul> <p><b>Example:</b> If you want to send a warning alert on matched text value "power off" and an error alert if more than one server is turned off, set the following thresholds:</p> <ul style="list-style-type: none"> <li>• Error if matchCount &gt; 1</li> <li>• Warning if value == 'power off'</li> </ul> <p>To send an error alert if only one threshold is matched, set Error if value == 'power off'.</p> <p>For details on how to create a Syslog monitor that triggers customized alerts for content matches, see <a href="#">"Customizing Syslog Content Matches and Monitor Alerts" on page 646</a>.</p> <ul style="list-style-type: none"> <li>• <b>Once, after all log entries have been checked.</b> 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>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>
<b>Process match</b>	<p>Expression describing the process to match in the log entries. You can also use a regular expression in this entry to match text patterns. The message entered here is displayed in the <b>Regular expression preview</b> box</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• If you enter more than 10 values for process or match messages, when you create a report by clicking the monitor title, the report includes only the first 10 values.</li> <li>• The /c search modifier is not supported.</li> </ul>
<b>Open Tool</b>	<p>Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.</p>



UI Element	Description
<b>Message match</b>	<p>Expression describing the message to match in the log entries. You can also use a regular expression in this entry to match text patterns. The message entered here is displayed in the <b>Regular expression preview</b> box.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The search is case sensitive.</li> <li>• If you enter more than 10 values for process or match messages, when you create a report by clicking the monitor title, the report includes only the first 10 values.</li> <li>• The /c search modifier is not supported.</li> </ul>
<b>Regular expression preview</b>	<p>Displays a preview of the regular expression text match to run which includes the text from the <b>Process match</b> and <b>Message match</b> boxes above.</p> <p>The Syslog monitor process and message 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><b>Note:</b> The regular expression cannot be changed on a monitor basis for the Syslog monitor. However, you can change the regular expression in <b>Infrastructure Preferences &gt; Custom Settings</b> under <b>System log match regular expression</b>.</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 the 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>
<b>Match value labels</b>	<p>Use 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 (,).</p> <p>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>

UI Element	Description
<b>Server-side processing</b>	<p>Processes 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 Syslog monitor is performing badly in regular mode).</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <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> <li>To enable server-side processing to work correctly when monitoring on a Solaris server, open the remote server settings for the monitored host (<b>Remote Servers &gt; UNIX Remote Servers &gt; Main Settings</b>), and enter a path to the bash interpreter in the <b>Initialize shell environment</b> field.</li> </ul>
<b>No error if file not found</b>	<p>Monitor remains 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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Limitations

- When monitoring a log file on a FreeBSD remote server, make sure the correct path to the "cat" command is used in **<SiteScope root directory>\templates.os/FreeBSD.config**, since the command was moved in the latest FreeBSD versions.
- SiteScope is unable to execute a command with more than 80 characters on a remote UNIX server via a Telnet connection (the "unable to read log file" message is displayed in the Syslog monitor summary). To avoid this issue, increase the COLUMNS variable in the UNIX shell script that is used to customize the shell environment (for bash this is .bashrc).
- When configuring this monitor in template mode, some fields that contain drop-down lists may be displayed as text boxes, and the **Browse Servers** and **Add Remote Server** buttons are not displayed.
- Log files with full name that contains **/dev/** folder are not displayed in the log file path list.

# Chapter 100: Tuxedo Monitor (Deprecated)

**Note:** The Tuxedo monitor was deprecated. If this monitor was configured in a previous version of SiteScope, it is still displayed in SiteScope after performing an upgrade (but will not work). This monitor is supported in SiteScope 11.24 and earlier versions.

Use the Tuxedo monitor to monitor the server performance data for Tuxedo 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. The error and warning thresholds for the monitor can be set on one or more Tuxedo monitor performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Tuxedo monitor.

## Learn About

### Supported Platforms/Versions

- This monitor supports monitoring server performance data for Oracle Tuxedo 6.5, 7.1, 8.0, 8.1, 9.0, and 9.1 servers.
- 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 monitor does not work with the 64-bit version of SiteScope, so if you plan to work with this monitor, it is recommended to install the SiteScope 32-bit version.

## Tasks

### How to Configure the Tuxedo Monitor

#### 1. Prerequisites

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.
- To get counter data on the Tuxedo monitor, user permissions/access control list (ACL) for the SiteScope Tuxedo monitor must be set on the Tuxedo server. For details, see ["Monitor Troubleshooting" on page 653](#).
- 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.

## 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## Tuxedo Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Basic Tuxedo Settings</b>	
<b>Server</b>	Name or IP address of the server. The address should match that dedicated to the Tuxedo Workstation component (the WSL process).  On UNIX servers, enter the full path of the applicable server.
<b>Port</b>	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>	User name if required to access the Tuxedo server.
<b>Password</b>	Password if required to access the Tuxedo server.
<b>Advanced Tuxedo Settings</b>	

UI Element	Description
<b>Client name</b>	Optional client name for the Tuxedo server.
<b>Connection data</b>	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>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<b>Server</b> <ul style="list-style-type: none"><li>• Requests per second</li><li>• Workload per second</li></ul> <b>Machine</b> <ul style="list-style-type: none"><li>• Workload completed per second</li><li>• Workload initiated per second</li></ul> <b>Queue</b> <ul style="list-style-type: none"><li>• Bytes on queue</li><li>• Messages on queue</li></ul>	<b>Workstation Handler (WSH)</b> <ul style="list-style-type: none"><li>• Bytes received per second</li><li>• Bytes sent per second</li><li>• Messages received per second</li><li>• Messages sent per second</li><li>• Number of queue blocks per second</li></ul>
--	--

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

### Monitor Troubleshooting

**Problem:** Counter data is not displayed for the Tuxedo monitor, and the following error is displayed:

Error 31008

Error getting counters: Failed to get browse data. Error Code: -1. Description:

Could not connect to application server. Reason: TPEPERM - bad permissions

[MsgId: MMSG-96006]

In addition, the Tuxedo log has:

```
155021.ecntest!AUTHSVR.1081376.1.0: CMDTUX_CAT:4130: INFO: Authentication failed for user test/  
155021.ecntest!WSH.2166972.1.0: LIBTUX_CAT:6249: ERROR: Unable to establish security context.  
Error code 270,
```

**Reason:** Tuxedo SECURITY ACL is enabled.

To get counter data on the Tuxedo monitor, user permissions/access control list (ACL) for the monitor must be set on the Tuxedo server. Tuxedo security requires the user name, user password and the application password ([http://docs.oracle.com/cd/E13203\\_01/tuxedo/tux80/atmi/secpgm7.htm](http://docs.oracle.com/cd/E13203_01/tuxedo/tux80/atmi/secpgm7.htm)).

**Solution:**

1. On the Tuxedo server, create a user without a password.
2. Configure the Tuxedo monitor in SiteScope:
  - In **Basic Tuxedo Settings**, enter a user name and for the password enter the application password.
  - In **Advanced Tuxedo Settings**, leave the **Client name** and **Connection data** fields empty.

When running the Tuxedo monitor, counter data should be displayed in SiteScope.

# Chapter 101: UDDI Monitor

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the UDDI monitor.

## License Consumption

Point-based Usage	Capacity-based Usage
One point per monitor	One OSi license per monitored host

## Tasks

### How to Configure the UDDI Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## UI Descriptions

### UDDI Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Inquiry URL</b>	UDDI server inquiry URL. <b>Example:</b> <code>http://uddi.company.com/inquiry/</code>
<b>Business name</b>	Business entity to search for in the UDDI server.
<b>Maximum number of businesses</b>	Maximum number of business entities to receive from the UDDI server (1–200). <b>Default value:</b> 10

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Chapter 102: UNIX Resources Monitor

The UNIX Resources monitor enables you to monitor multiple system statistics on a single UNIX system.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the UNIX Resources monitor.

## Learn About

This section includes:

- ["UNIX Resources Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)
- ["Server-Centric Report" on the next page](#)
- ["License Usage" on the next page](#)

## 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 error and warning thresholds for the monitor can be set on one or more server system statistics.

The UNIX Resources monitor queries the list of UNIX servers currently configured in the UNIX Remote Servers container.

## Supported Platforms/Versions

This monitor supports monitoring UNIX remote servers running on:

- Solaris 2.7, 2.8, 2.9, 5.10, 7, 8, 9, 10, 10 8/11 ("U10"), 10 1/13 ("U11"), 11, 11.2
- Red Hat Linux 7.x, 8.x, 9.x
- Red Hat Linux AS/ES Linux 3.x, 4.x, 5.2, 5.4 - 5.10, 6.0 - 6.5, 7
- Oracle Enterprise Linux 6.4, 6.5, 7.0
- 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
  - HP-UX 11i v3
- AIX 5.2, 5.3, 6.1, 7.0, 7.1

**Note:** The UNIX Resources monitor does not support monitoring remote servers running on HP NonStop



operating systems; use the ["HP NonStop Resources Monitor" on page 306](#) instead.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SSH protocol only.

**Note:** SSH is supported only when SiteScope is installed on UNIX machines.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## 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 SiteScope Dashboard. For details, see Creating Server-Centric Reports in the Using SiteScope Guide.

## License Usage

Points-based Usage	Capacity-based Usage
One point per instance Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

# Tasks

## How to Configure the UNIX Resources Monitor

### 1. Prerequisites

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 How to Configure SiteScope to Monitor a Remote UNIX Server in the Using SiteScope Guide.

### 2. Configure the monitor properties


Configure the monitor properties as required.


For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## UNIX Resources Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of the server that you want to monitor. Select a server from the server list (only those UNIX 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:</b> To avoid a timeout when monitoring a UNIX remote server using an SSH connection (if the external drives mounted by NFS are unavailable for the target remote), use the "umount -a -t nfs" command to unmount all NFS drives, or use "umount -n &lt;nodename&gt;" to unmount all the drives from the particular remote node that is unavailable. Use the "mount   grep nfs" command to get a list of NFS drives.</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) Name of any SiteScope remote server from which you want to get counters.
<b>Add Remote Server</b>	Opens the Add UNIX Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit UNIX Remote Server Dialog Box in the Using SiteScope Guide.
<b>Available Counters</b>	<p>Displays the available measurements for this monitor.</p> <p>For each measurement, select the <b>Object</b>, <b>Instances</b> and <b>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> <p><b>Note:</b> The Disk Stat counter is available only when monitoring remote servers running on Linux version 2.4. This is because the <b>/proc/stat/</b> command, which retrieves relevant disk stat information, is available for this version only.</p> <p>For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</p> <p><b>Note:</b> Objects are no longer automatically updated after opening the monitor's properties. Instead, click the <b>Reload Objects</b> button to reload data for the selected objects.</p>
<b>Reload Objects</b>	Reloads data for the selected objects.

UI Element	Description
<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>
<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 Server-Centric Report in the Using SiteScope Guide.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<ul style="list-style-type: none"> <li>• Block device activity</li> <li>• Buffer activity</li> <li>• CPU utilization</li> <li>• Cache stats</li> <li>• Console keyboard</li> <li>• Console mouse</li> <li>• Disk errors</li> <li>• Disk partition</li> <li>• File access system routines</li> <li>• File systems</li> <li>• Inode cache</li> <li>• Kernel network stats</li> <li>• Kernel memory allocation (KMA) activities</li> <li>• Load average</li> <li>• Memory</li> </ul>	<ul style="list-style-type: none"> <li>• Message and semaphore activities</li> <li>• NFS client</li> <li>• NFS server</li> <li>• Network interface</li> <li>• Paging activity</li> <li>• Physical disk</li> <li>• Process</li> <li>• Process (Complete Name) - retrieves long names for processes &gt; 80 characters</li> <li>• Processor</li> <li>• Processor info</li> <li>• Queue length</li> <li>• RPC client</li> <li>• RPC server</li> <li>• Status of process and inode file tables</li> <li>• System info</li> <li>• System calls</li> </ul>
---	--

## Tips/Troubleshooting

### General Notes/Limitations

- When configuring this monitor in template mode, you can use regular expressions to define counters.
- When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- To avoid a timeout when monitoring a UNIX remote server using an SSH connection (if the external drives mounted by NFS are unavailable for the target remote), use the "umount -a -t nfs" command to unmount all NFS drives, or use "umount -n <nodename>" to unmount all the drives from the particular remote node that is unavailable. Use the "mount | grep nfs" command to get a list of NFS drives.
- After upgrading to SiteScope 11.23, all counters of the Object Processor info list return "n/a" if they were

installed in previous versions, because instances for the counters were added.

**Solution:** Reinstall all counters of the UNIX Resources monitor Processor info list by clicking the **Reload Objects** button.

- Incorrect CPU cores number is given when you run this monitor on an AIX operating system using multiple cores when CPU utilization is low, and simultaneous multithreading (SMT) is on.

**Cause:** If SMT is on (it is on by default in AIX), the CPU cores number will be multiplied by 2 or 4 depending on the hardware model and/or partition mode.

**Solution:** Turn SMT to off.

- The following error is displayed in the monitor summary when monitoring a UNIX remote server running on a Solaris (SunOS) operating system: "Command parser getCurrentData() returned null, it means we had some sort of connection problem: [ Monitor ID = null, Parser Name = Kstat Network Interface]".

**Cause:** The default secure shell (SSH) command to be run on the remote server has reached the maximum number of characters.

**Solution:** Initialize bash shell in the remote UNIX (Solaris) server settings. To do so, open the UNIX remote server used to monitor the Solaris Sun operating system, and enter `/bin/bash` in the **Initialize shell environment** field for the UNIX remote server.

- To enable the UNIX Resources monitor to retrieve Network Interface object counters when monitoring a remote Solaris server, you need to enter the command `/bin/bash` in the **Initialize shell environment** field of the UNIX Remote Server settings. This enables the monitor to get counters for **vnet\***, **eri\***, **qfe\***, **ce\***, **bge\***, **xge\***, and **e1000g\*** network adapters (NICs).
- When monitoring a UNIX remote server running on a Linux operating system with a non-english locale, the monitor is unable to get counters for file systems or inode cache objects.

**Solution:** Enter `export LANG=en_EN.UTF-8` in the **Initialize shell environment** field for the UNIX remote server.

# Chapter 103: URL Monitor

This monitor provides 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the URL monitor.

## Learn About

This section includes:

- ["URL Monitor Overview" below](#)
- ["Supported Platforms/Versions" on the next page](#)
- ["What to Monitor" on the next page](#)
- ["Status" on the next page](#)
- ["Scheduling the Monitor" on the next page](#)
- ["Support for IPv6 Addresses" on page 663](#)
- ["SSL Connectivity" on page 663](#)
- ["License Consumption" on page 663](#)

## URL Monitor Overview

The URL monitor is used to monitor a specified Web page to verify that it can be retrieved. 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.

## Supported Platforms/Versions

The URL monitor supports monitoring HTTP versions 1.0 and 1.1.

## 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 use 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 SiteScope 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 good.

## 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.

## Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP and HTTPS protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## 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 Monitor" on page 661](#).
- Importing the server certificate. For details on how to perform this task, see ["How to Configure the URL Monitor" on the next page](#).

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol/HTTP Client used by SiteScope	Java ("Use WinInet" is not selected)	WinInet ("Use WinInet" is selected)
SSLv2	x	x
SSLv3	√	√
TLSv1.0, TLSv1.1, TLSv1.2	√	√

## License Consumption

Points-based Usage	Capacity-based Usage
One point per URL	One URL license per monitored link

# Tasks

This section includes:

- ["How to Configure the URL Monitor" below](#)
- ["How to Manually Import Server Certificates " below](#)

## How to Configure the URL Monitor

### 1. Prerequisites

The user name and password specified in the **Credentials** section (in **Authentication Settings**) must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.

### 2. 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 [How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide](#).
- Import the server certificates manually. For details, see ["How to Manually Import Server Certificates " below](#).

### 3. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

#### Tip:

- The **URL Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see [URL Tool in the Using SiteScope Guide](#).
- 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.

## How to Manually Import Server Certificates

Instead of using Certificate Management, you can manually import certificates 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 in the Using SiteScope Guide](#).

### 1. Check the certificates already in the keystore, from the **<SiteScope root directory>\javallib\security** directory, by entering:

```
../../bin/keytool -list -keystore cacerts
```

### 2. Import the certificate, into **<SiteScope root directory>\javallib\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.

## UI Descriptions

### URL Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>URL</b>	<p>URL that you want to monitor.</p> <p><b>Example:</b> <code>http://demo.thiscompany.com</code></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> <code>https://www.thiscompany.com</code></p>
<b>Match content</b>	<p>Text string to match in the returned page or frameset. If the text is not contained in the page, the monitor displays the message <code>content match error</code>. The search is case sensitive.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"><li>• 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. For example, <code>&lt; B&gt; Hello&lt; /B&gt; World</code>.</li><li>• You can also perform a regular expression match by enclosing the string in forward slashes, with a letter <code>i</code> after the trailing slash indicating case-insensitive matching. For example, <code>/href=Doc\d+\.html/</code> or <code>/href=doc\d+\.html/i</code>.</li><li>• You can search for a pattern string across multiple lines. To do so, add the <code>/s</code> modifier to the end of the regular expression. For example, <code>/(state).*(populate)/s</code> checks if the returned page contains both "state" and "populate".</li></ul> <p>For details on regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.</p>

UI Element	Description
<b>Open Tool</b>	Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.
<b>Match content for error</b>	<p>Text string 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><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 in the Using SiteScope Guide.</li> <li>• HTML tags are part of a text document, so include them if they are part of the text for which you are searching. For example, &lt; B&gt; Error &lt; /B&gt; Message.</li> <li>• You can also perform a regular expression match by enclosing the string in forward slashes, with an i after the trailing slash indicating case-insensitive matching. For example, /href=Doc\d+\.html/ or /href=doc\d+\.html/i.</li> </ul>
<b>Show detailed measurement</b>	<p>Records 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 for all page components. It is calculated using the formula:  <math display="block">\text{Response time} = [\text{Time when SiteScope received first byte of response}] - [\text{Time when SiteScope sent GET request}] +</math> <math display="block">[\text{Time when SiteScope received first byte of response for image/frame 1}] - [\text{Time when SiteScope sent GET request for image/frame 1}] +</math> <math display="block">[\text{Time when SiteScope received first byte of response for image/frame n}] - [\text{Time when SiteScope sent GET request for image/frame n}]</math> </li> <li>• <b>Download time.</b> The time it takes to download the entire page.</li> </ul>
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, to 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>

UI Element	Description
<b>Retries</b>	<p>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>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>
<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 Set-cookie: cookieName=cookieValue.</p> <p>To change the content type of a post, use the format Content-Type: application/my-format.</p> <p>To substitute 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> <p>POST data can be used to add headers. While using POST data field to add headers, you should specify the header names in the POST data field only. Do NOT specify the headers in the Request headers field while using POST data field.</p>

UI Element	Description
<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> Encodes the POST data by the content type header. If the header equals <code>urlencoded</code> then encode, otherwise do not encode.</li> <li>• <b>Force URL encoding.</b> Always encodes the post data.</li> <li>• <b>Do not force URL encoding.</b> Does not encode the POST data.</li> </ul>
<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 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>
<b>Error if redirected</b>	<p>Generates an error (and notifies you) if a URL is redirected.</p> <p><b>Default value:</b> Not selected</p>
<b>HTTP version</b>	<p>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>
<b>Retrieve images</b>	<p>The status and response time statistics 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 retrieved only once.</p> <p><b>Note:</b> If this option is checked, each image referenced by the target URL contributes to the response and 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>

UI Element	Description
<b>Retrieve frames</b>	<p>Retrieves the frames references in a frameset and counts 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 response and 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>Use WinInet</b>	<p>WinInet is used as an alternative HTTP client for this monitor.</p> <p>Select this option to use WinInet instead of Java (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 such as SSLv3, 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> <p><b>Note:</b> WinInet functionality is available on Windows versions of SiteScope only. For troubleshooting WinInet functionality, see <a href="#">"Problems Using WinInet" on page 672</a>.</p>
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URL.
<b>Proxy server user name</b>	<p>Proxy server user name if the proxy server requires a user name to access the URL.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy server password</b>	<p>Proxy serverpassword if the proxy server requires a user name to access the URL.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy NTLM V2</b>	Select if the proxy requires authentication using NTLM version 2.
<b>Authentication Settings</b>	

UI Element	Description
<b>Credentials</b>	<p>Option to use for authorizing credentials if the URL specified requires a name and password for access:</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 How to Configure Credential Preferences in the Using SiteScope Guide.</li> </ul>
<b>Pre-emptive authorization</b>	<p>Option for sending authorization credentials 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.</li> </ul> <p><b>Note:</b> If the URL does not require a user name and password, this option may cause the URL to fail.</p> <ul style="list-style-type: none"> <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.</li> </ul> <p><b>Note:</b> If the URL does not require a user name and password, this option may be used.</p> <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>Client side certificate</b>	<p>The certificate file, if you need to use a client side certificate to access the target URL. 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>Password if you are using a client side certificate and that certificate requires a password.</p>
<b>Authorization NTLM domain</b>	<p>Domain for NT LAN Manager (NTLM) authorization if required to access the URL.</p>

UI Element	Description
<b>Accept untrusted certificates for HTTPS</b>	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 <a href="#">"SSL Connectivity" on page 663</a> .
<b>Accept invalid certificates for HTTPS</b>	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.
<b>NTLM V2</b>	Select if the URL you are accessing requires authentication using NTLM version 2.
<b>Preferred protocols</b>	<p>Select the preferred protocol option to use for the handshake process.</p> <ul style="list-style-type: none"> <li>• <b>Any supported protocol.</b> Enables any supported protocol to be used for the handshake process (this is the default setting). Since this option uses SSL protocols, SSL must be enabled on the Web server to use this option.</li> <li>• <b>Prefer SSL to TLS.</b> Select if the URL you are accessing cannot handle authentication using TLS. This enables encrypted handshake messages to be sent using SSL. <b>Note:</b> This option is ignored (if selected) when SiteScope is running in FIPS 140-2 mode, since authentication using TLS is mandatory with FIPS 140-2. For details on FIPS 140-2, see the Running SiteScope Securely section of the SiteScope Deployment Guide (&lt;SiteScope root directory&gt;\sisdocs\doc_lib\Get_Documentation.htm).</li> <li>• <b>Prefer TLS to SSL.</b> Select if you prefer to use TLS for encrypting handshake messages or if the URL you are accessing cannot handle authentication using SSL. TLS is the latest cryptographic protocol. TLS 1.0, 1.1, and 1.2 are supported.</li> <li>• <b>Prefer TLSv1.0.</b> Select if you prefer to use only the TLS 1.0 version.</li> <li>• <b>Prefer TLSv1.1.</b> Select if you prefer to use only the TLS 1.1 version.</li> <li>• <b>Prefer TLSv1.2.</b> Select if you prefer to use only the TLS 1.2 version.</li> </ul>

## Monitor Counters

Below is the list of counters for this monitor:

- **age (seconds)** - Amount of time, in seconds, it took for the page to complete downloading.
- **certificate expiration days remaining** - Number of days to the earliest expiration date of any certificate in the chain of certificate that was used to establish the SSL connection.
- **content match** - Displays the text string to match in the returned page or frameset.
- **overall status** - Relates to HTTP status codes in the page and in components of the page such as images or frames.
- **round trip time (milliseconds)** - Amount of time to complete the following: (1). Name lookup, DNS (2). Connect to the server socket (3). Send the HTTP request (4). Download the entire page. While this counter is measured in milliseconds in the Threshold Settings, it is displayed in seconds in the SiteScope Dashboard.
- **size (bytes)** - The current page size of the URL in bytes.

- status - Relates only to HTTP status codes (such as 200, 302, and 404) in the page itself.
- total errors (errors) - The total number of errors encountered downloading the page.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and limitations:

- ["General Notes/Limitations" below](#)
- ["Problems Using WinInet" below](#)
- ["Error Messages" on the next page](#)

### General Notes/Limitations

- While the **round trip time** performance counter is measured in milliseconds in the Threshold Settings, it is displayed in seconds in the SiteScope Dashboard.
- When SiteScope is connected to BSM, not all monitor metrics are reported to BSM. If a URL monitor gets its status from a metric that is not reported to BSM and a metric that is reported to BSM (for example, **roundtrip time**) does not have any threshold set in SiteScope, then no monitor status is reported to BSM.
- When setting thresholds for the URL monitor, the **status** condition relates only to HTTP status codes (such as 200, 302, and 404) in the page itself, whereas **overall status** relates to HTTP status codes in the page and in components of the page such as images or frames (provided **Retrieve images** and **Retrieve frames** are selected in the monitor settings).
- When using several URL load threads, the total duration time might be less than the combined total of the DNS lookup, connection, server response, and download time. In this case, total duration time is the duration between the start and end of all threads, whereas DNS lookup, connection, response, and download time is the sum of the corresponding value of each thread. You can set the required count of URL load threads in the **\_urlLoadThreads** property in **<SiteScope root directory>\groups\master.config**.

### Problems Using WinInet

Check the WinInet flow:

- Try to reach your URL in Internet Explorer by opening it in command prompt:  

```
$ runas /user:DOMAIN\USER_NAME "C:\Program Files\Internet Explorer\iexplore.exe /separate"
```

where DOMAIN\USER\_NAME is account of a user under which SiteScope is running,  
If you cannot open the URL, try to analyze why.
- Check for server certificate revocation. If you encounter HTTP Error 12057 (which indicates that revocation cannot be checked because the revocation server is offline), either:
  - Avoid using WinInet, or
  - In Internet Explorer, select **Tools > Internet Options > Advanced > Security**, and switch off **Check for server certificate revocation**.



- Other common problems:
  - Not enough user permissions
  - Cookies are blocked (indicated by a 403 Forbidden error)

## Error Messages

The following error codes might be encountered when working with URL monitors.

Error Code	Description and Troubleshooting
(-982)	Permission denied.
(-983)	SOAP Fault Error.
(-986)	This message is returned when an item is not found in the XML content. Check the XML content by using the <b>View Source</b> command from a browser.
(-987)	This message is returned when a syntax problem is found in the XML content. Check the XML content by using the <b>View Source</b> command from a browser.
(-988)	This message is returned when the value of an item in an XML document is incorrect. Check the XML content by using the <b>View Source</b> command from a browser.
(-989)	This message is returned when an error string is found in the HTML content. Check the HTML content by using the <b>View Source</b> command from a browser.
(-990)	This message is returned when a link, form, or frame is not found in the HTML on a page. Check the HTML content for that step by using the <b>View Source</b> command from a browser.
(-991)	This message is returned when the server returns an incomplete response. It may be caused by a busy server or network. It may also be caused by a problem in a CGI script. Check the URL using a browser for additional information. Check the load on the network. Check the load on the server.
(-992)	Monitor Specific Error.
(-993)	This message is returned when there is not a network path that reaches the server. Check the network connection to the server. Check that firewalls and routers allow access to the server. Check the load on the network. Check that the server is running.
(-994)	This message is returned when a Windows library has an internal problem. If this problem occurs repeatedly, report it to your system administrator.
(-995)	This message is returned when the content of a URL changes. Check the URL using a browser to view the new contents.
(-996)	This message is returned when a connection is made but not completed. Check the load on the network. Check the load on the server.

Error Code	Description and Troubleshooting
(-997)	This message is returned when DNS cannot find an IP address for a name. Check the network connection to the DNS server. Check that the DNS server for that domain is running. Check that DNS is properly configured on the SiteScope machine. Check that the name exists in the configuration for that domain.
(-998)	This message is returned when the server does not accept the connection. Check that the server and server process are running. Check the load on the server. Check the load on the network.
(-999)	This message is returned when the match string is not found in the HTML content. Check the HTML content by using the View Source command from a browser.
(-1000)	URL Unknown Error.
(-1001)	IP address does not match.
(-1002)	Unable to connect to remote monitoring server.
(-1003)	This message is returned when connection was reset. Check the URL using a browser for additional information. Check the load on the network. Check the load on the server.
(12157)	Insufficient encryption, probably needs 128 bit Internet Explorer.
(12037)	Secure certificate has expired.
(12038)	Secure certificate name does not match host name.
(12044)	Requires client certificate authentication.
(12045)	Certificate authority not registered in SiteScope cacerts file.
(12046)	URL Certificate Peer Error.

# Chapter 104: URL Content Monitor

The URL Content monitor is a specialized variation of the ["URL Monitor" on page 661](#) 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the URL Content monitor.

## Learn About

This section includes:

- ["URL Content Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Status" below](#)
- ["Support for IPv6 Addresses" on the next page](#)
- ["SSL Connectivity" on the next page](#)
- ["License Consumption" on page 677](#)

## 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.

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.

## Supported Platforms/Versions

The URL Content monitor supports monitoring HTTP versions 1.0 and 1.1.

## 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 SiteScope Dashboard dependent on the results of the retrieval, content match, and the error or warning status criteria that you select.

## Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP and HTTPS protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## 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 678](#).
- Importing the server certificate. For details on how to perform this task, see ["How to Configure the URL Content Monitor" on the next page](#).

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol/HTTP Client used by SiteScope	Java ("Use WinInet" is not selected)	WinInet ("Use WinInet" is selected)
SSLv2	x	x
SSLv3	√	√
TLSv1.0, TLSv1.1, TLSv1.2	√	√

## License Consumption

Points-based Usage	Capacity-based Usage
1 point per monitor	One URL license per monitored URL

## Tasks

This section includes:

- ["How to Configure the URL Content Monitor" below](#)
- ["How to Manually Import Server Certificates" below](#)

### How to Configure the URL Content Monitor

#### 1. Prerequisites

The user name and password specified in the **Credentials** section (in **Authentication Settings**) must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.

#### 2. 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 [How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide](#).
- Import the server certificates manually. For details, see ["How to Manually Import Server Certificates" below](#).

#### 3. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the [UI Descriptions](#) section below.

**Tip:** The **URL Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see [URL Tool in the Using SiteScope Guide](#).

### How to Manually Import Server Certificates

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 Overview in the Using SiteScope Guide](#).

#### 1. Check the certificates already in the keystore, from the **<SiteScope root directory>\javallib\security** directory, by entering:

```
../../bin/keytool -list -keystore cacerts
```

#### 2. Import the certificate, into **<SiteScope root directory>\javallib\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, 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.

## UI Descriptions

### URL Content Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>URL</b>	<p>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>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 enable 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>
<b>Open Tool</b>	<p>Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.</p>

UI Element	Description
<b>Match content labels</b>	<p>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 <code>Copyright_start</code>, <code>Copyright_end</code> 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. SiteScope also sends the label name of content matches to Generic Data integrations, Diagnostics integrations, and OM metrics integrations.</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>Text string to check for in the returned page. If the text is contained in the page, the monitor displays <code>content error found</code>. 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> <code>&lt; B&gt; Error &lt; /B&gt; Message</code></p> <p>You can also perform a regular expression match by enclosing the string in forward slashes, with an <code>i</code> 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 in the Using SiteScope Guide.</p> <p><b>Example:</b> <code>/href=Doc\d+\.html/</code> or <code>/href=doc\d+\.html/i</code></p> <p><b>Note:</b> The search is case sensitive.</p>
<b>Show detailed measurement</b>	<p>SiteScope records 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>Amount of time, in seconds, to 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>

UI Element	Description
<b>Retries</b>	<p>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>HTTP Settings</b>	
<b>Request headers</b>	<p>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> <p>POST data can be used to add headers. While using POST data field to add headers, you should specify the header names in the POST data field only. Do NOT specify the headers in the Request headers field while using POST data field.</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>



UI 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>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>
<b>Retrieve images</b>	<p>The status and response time statistics 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>Retrieves the frames references in a frameset and counts 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>SiteScope notifies you if a URL is redirected.</p>

UI Element	Description
<b>Use WinInet</b>	<p>WinInet is used as an alternative HTTP client for this monitor.</p> <p>Select this option to use WinInet instead of Java (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 such as SSLv3, 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> WinInet functionality is available on Windows versions of SiteScope only. For troubleshooting WinInet functionality, see <a href="#">"Problems Using WinInet" on page 685</a>.</p>
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URL.
<b>Proxy server user name</b>	<p>Proxy server user name if required to access the URL.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy server password</b>	<p>Proxy server password if required to access the URL.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy NTLM V2</b>	Proxy requires authentication using NTLM version 2.
<b>Authentication Settings</b>	
<b>Credentials</b>	<p>Option to use for authorizing credentials if the URL specified requires a name and password for access:</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 How to Configure Credential Preferences in the Using SiteScope Guide.</li> </ul>

UI Element	Description
<b>Pre-emptive authorization</b>	<p>Option for sending authorization credentials 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.</li> </ul> <p><b>Note:</b> If the URL does not require a user name and password, this option may cause the URL to fail.</p> <ul style="list-style-type: none"> <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.</li> </ul> <p><b>Note:</b> If the URL does not require a user name and password, this option may be used.</p> <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 <a href="#">"SSL Connectivity" on page 676</a>.</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>
<b>Client side certificates</b>	<p>Certificate file if you need to use a client side certificate to access the target URL. 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>Password for a client side certificate if required.</p>
<b>Authorization NTLM domain</b>	<p>Domain for NT LAN Manager (NTLM) authorization if 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>

UI Element	Description
<b>Preferred protocols</b>	<p>Select the preferred protocol option to use for the handshake process.</p> <ul style="list-style-type: none"> <li>• <b>Any supported protocol.</b> Enables any supported protocol to be used for the handshake process (this is the default setting). Since this option uses SSL protocols, SSL must be enabled on the Web server to use this option.</li> <li>• <b>Prefer SSL to TLS.</b> Select if the URL you are accessing cannot handle authentication using TLS. This enables encrypted handshake messages to be sent using SSL. <b>Note:</b> This option is ignored (if selected) when SiteScope is running in FIPS 140-2 mode, since authentication using TLS is mandatory with FIPS 140-2. For details on FIPS 140-2, see the Running SiteScope Securely section of the SiteScope Deployment Guide (&lt;SiteScope root directory&gt;\sisdocs\doc_lib\Get_Documentation.htm).</li> <li>• <b>Prefer TLS to SSL.</b> Select if you prefer to use TLS for encrypting handshake messages or if the URL you are accessing cannot handle authentication using SSL. TLS is the latest cryptographic protocol. TLS 1.0, 1.1, and 1.2 are supported.</li> <li>• <b>Prefer TLSv1.0.</b> Select if you prefer to use only the TLS 1.0 version.</li> <li>• <b>Prefer TLSv1.1.</b> Select if you prefer to use only the TLS 1.1 version.</li> <li>• <b>Prefer TLSv1.2.</b> Select if you prefer to use only the TLS 1.2 version.</li> </ul>

## Monitor Counters

Below is the list of counters for this monitor:

- age (seconds) - Amount of time, in seconds, it took for the page to complete downloading.
- certificate expiration days remaining - Number of days to the earliest expiration date of any certificate in the chain of certificate that was used to establish the SSL connection.
- content match - Displays the text string to match in the returned page or frameset.
- overall status - Relates to HTTP status codes in the page and in components of the page such as images or frames.
- round trip time (milliseconds) - Amount of time to complete the following: (1). Name lookup, DNS (2). Connect to the server socket (3). Send the HTTP request (4). Download the entire page. While this counter is measured in milliseconds in the Threshold Settings, it is displayed in seconds in the SiteScope Dashboard.
- size (bytes) - The current page size of the URL in bytes.
- status - Relates only to HTTP status codes (such as 200, 302, and 404) in the page itself.
- total errors (errors) - The total number of errors encountered downloading the page.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- age (seconds) - Amount of time, in seconds, it took for the page to complete downloading.
- certificate expiration days remaining - Number of days to the earliest expiration date of any certificate in the chain of certificate that was used to establish the SSL connection.
- connect time (milliseconds) - Amount of time, in milliseconds, it took to connect to the page.

- content match - Displays the text string to match in the returned page or frameset.
- deviation percentage (connect time %)
- deviation percentage (dns time %)
- deviation percentage (download time %)
- deviation percentage (response time %)
- deviation percentage (roundtrip time %)
- dns time (milliseconds) - Displays the amount of time, in milliseconds, it took to resolve the DNS name to an IP address.
- download time (milliseconds) - Displays the time it took to download the entire page.
- overall status - Relates to HTTP status codes in the page and in components of the page such as images or frames.
- response time (milliseconds)
- round trip time (milliseconds) - Amount of time to complete the following: (1). Name lookup, DNS (2). Connect to the server socket (3). Send the HTTP request (4). Download the entire page. While this counter is measured in milliseconds in the Threshold Settings, it is displayed in seconds in the SiteScope Dashboard.
- size (bytes) - The current page size of the URL in bytes.
- status - Relates only to HTTP status codes (such as 200, 302, and 404) in the page itself.
- total errors (errors) - The total number of errors encountered downloading the page.

## Tips/Troubleshooting

This section describes troubleshooting and limitations:

- ["General Notes/Limitations" below](#)
- ["Problems Using WinInet" below](#)
- ["Error Messages" on the next page](#)

### General Notes/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.
- When using several URL load threads, the total duration time might be less than the combined total of the DNS lookup, connection, server response, and download time. In this case, total duration time is the duration between the start and end of all threads, whereas DNS lookup, connection, response, and download time is the sum of the corresponding value of each thread. You can set the required count of URL load threads in the `_urlLoadThreads` property in **<SiteScope root directory>\groups\master.config**.

### Problems Using WinInet

Check the WinInet flow:

- Try to reach your URL in Internet Explorer by opening it in command prompt:  

```
$ runas /user:DOMAIN\USER_NAME "C:\Program Files\Internet Explorer\iexplore.exe /separate"
```

where DOMAIN\USER\_NAME is account of a user under which SiteScope is running,

If you cannot open the URL, try to analyze why.

- Check for server certificate revocation. If you encounter HTTP Error 12057 (which indicates that revocation cannot be checked because the revocation server is offline), either:
  - Avoid using WinInet, or
  - In Internet Explorer, select **Tools > Internet Options > Advanced > Security**, and switch off **Check for server certificate revocation**.
- Other common problems:
  - Not enough user permissions
  - Cookies are blocked (indicated by a 403 Forbidden error)

## Error Messages

The following error codes might be encountered when working with URL monitors.

Error Code	Description and Troubleshooting
(-982)	Permission denied.
(-983)	SOAP Fault Error.
(-986)	This message is returned when an item is not found in the XML content. Check the XML content by using the <b>View Source</b> command from a browser.
(-987)	This message is returned when a syntax problem is found in the XML content. Check the XML content by using the <b>View Source</b> command from a browser.
(-988)	This message is returned when the value of an item in an XML document is incorrect. Check the XML content by using the <b>View Source</b> command from a browser.
(-989)	This message is returned when an error string is found in the HTML content. Check the HTML content by using the <b>View Source</b> command from a browser.
(-990)	This message is returned when a link, form, or frame is not found in the HTML on a page. Check the HTML content for that step by using the <b>View Source</b> command from a browser.
(-991)	This message is returned when the server returns an incomplete response. It may be caused by a busy server or network. It may also be caused by a problem in a CGI script. Check the URL using a browser for additional information. Check the load on the network. Check the load on the server.
(-992)	Monitor Specific Error.

Error Code	Description and Troubleshooting
(-993)	This message is returned when there is not a network path that reaches the server. Check the network connection to the server. Check that firewalls and routers allow access to the server. Check the load on the network. Check that the server is running.
(-994)	This message is returned when a Windows library has an internal problem. If this problem occurs repeatedly, report it to your system administrator.
(-995)	This message is returned when the content of a URL changes. Check the URL using a browser to view the new contents.
(-996)	This message is returned when a connection is made but not completed. Check the load on the network. Check the load on the server.
(-997)	This message is returned when DNS cannot find an IP address for a name. Check the network connection to the DNS server. Check that the DNS server for that domain is running. Check that DNS is properly configured on the SiteScope machine. Check that the name exists in the configuration for that domain.
(-998)	This message is returned when the server does not accept the connection. Check that the server and server process are running. Check the load on the server. Check the load on the network.
(-999)	This message is returned when the match string is not found in the HTML content. Check the HTML content by using the View Source command from a browser.
(-1000)	URL Unknown Error.
(-1001)	IP address does not match.
(-1002)	Unable to connect to remote monitoring server.
(-1003)	This message is returned when connection was reset. Check the URL using a browser for additional information. Check the load on the network. Check the load on the server.
(12157)	Insufficient encryption, probably needs 128 bit Internet Explorer.
(12037)	Secure certificate has expired.
(12038)	Secure certificate name does not match host name.
(12044)	Requires client certificate authentication.
(12045)	Certificate authority not registered in SiteScope cacerts file.
(12046)	URL Certificate Peer Error.

# Chapter 105: URL List Monitor

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the URL List monitor.

## Learn About

This section includes:

- ["URL List Monitor Overview" below](#)
- ["Supported Platforms/Versions" below](#)
- ["Scheduling the Monitor" below](#)
- ["Support for IPv6 Addresses" on the next page](#)
- ["SSL Connectivity" on the next page](#)
- ["License Consumption" on page 690](#)

### 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" on page 347](#)) or other Web transaction processes (see ["URL Sequence Monitor" on page 697](#)).

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.

### Supported Platforms/Versions

The URL List monitor supports monitoring HTTP versions 1.0 and 1.1.

### Scheduling the Monitor

This is 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.

## Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP and HTTPS protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## 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 importing the server certificate. For details on how to perform this task, see ["How to Configure the URL List Monitor" on the next page](#).

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol/HTTP Client used by SiteScope	Java ("Use WinInet" is not selected)	WinInet ("Use WinInet" is selected)
SSLv2	x	x

Protocol/HTTP Client used by SiteScope	Java ("Use WinInet" is not selected)	WinInet ("Use WinInet" is selected)
SSLv3	√	√
TLSv1.0, TLSv1.1, TLSv1.2	√	√

## License Consumption

Points-based Usage	Capacity-based Usage
One point per URL	One URL license per monitored URL

## Tasks

This section includes:

- ["How to Configure the URL List Monitor" below](#)
- ["How to Manually Import Server Certificates" below](#)

### How to Configure the URL List Monitor

#### 1. Prerequisites

The user name and password specified in the **Credentials** section (in **Authentication Settings**) must have sufficient permissions to complete the HTTP request that the monitor is configured to perform.

#### 2. 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 [How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide](#).
- Import the server certificates manually. For details, see ["How to Manually Import Server Certificates" below](#).

#### 3. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the [UI Descriptions](#) section below.

### How to Manually Import Server Certificates

Instead of using Certificate Management, you can manually import certificates 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 in the Using SiteScope Guide](#).

1. Check the certificates already in the keystore, from the **<SiteScope root directory>\javallib\security** directory, by entering:  

```
../../bin/keytool -list -keystore cacerts
```
2. Import the certificate, into **<SiteScope root directory>\javallib\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.

## UI Descriptions

### URL List Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>URL list file</b>	<p>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. If the URLs are stored in a map format, each URL must be in the format:</p> <p><code>&lt;URL ID&gt;;&lt;host&gt;;&lt;port&gt;;&lt;secure&gt; or &lt;nonsecure&gt;;&lt;page&gt;</code></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>
<b>Log file</b>	<p>Path for the log file for this monitor. For each URL checked, an entry is added to this log file.</p> <p>If this item is blank, a log is not created.</p>
<b>Error log file</b>	<p>Path for the error log file for this monitor. For each error retrieving a URL, an entry is added to this log file.</p> <p>If this item is blank, a log is not created.</p>

UI Element	Description
<b>Specific server</b>	<p>Server name of URLs to check in the URL list. If the URLs are stored in a map format (see <b>URL list file</b> box for details), this item is used to check a subset of the URLs from the list.</p> <p><b>Default value:</b> All URLs that are in the list are checked.</p> <p><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.</p>
<b>Pause (milliseconds)</b>	<p>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.</p> <p><b>Default value:</b> 1000 milliseconds</p>
<b>Threads</b>	<p>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.</p> <p><b>Default value:</b> 4</p>
<b>Timeout (seconds)</b>	<p>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><b>Default value:</b> 60 seconds</p>
<b>Retries</b>	<p>Number of times you want SiteScope to try to reach URLs that are returning an error.</p> <p><b>Default value:</b> 0</p>
<b>HTTP Settings</b>	
<b>Request headers</b>	<p>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>WinInet is used as an alternative HTTP client for this monitor.</p> <p>Select this option to use WinInet instead of Java (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 such as SSLv3, 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> <p><b>Note:</b> WinInet functionality is available on Windows versions of SiteScope only. For troubleshooting WinInet functionality, see <a href="#">"Problems Using WinInet" on page 694</a>.</p>

UI Element	Description
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URLs in the list.
<b>Proxy server user name</b>	Proxy server user name if the required to access the URL. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	Proxy server password if the required to access the URL. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Authentication Settings</b>	
<b>Credentials</b>	Option to use for authorizing credentials if the URLs in the list require a user name and password for access: <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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>

## Monitor Counters

Below is the list of counters for this monitor:

- duration - The average amount of time in seconds, to retrieve the URLs.
- errors - The number of URLs that encountered an error.
- left - The number of URLs that have not yet been monitored.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and limitations:

- ["General Notes/Limitations" below](#)
- ["Problems Using WinInet" on the next page](#)
- ["Error Messages" on the next page](#)

### General Notes/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.

- When using several URL load threads, the total duration time might be less than the combined total of the DNS lookup, connection, server response, and download time. In this case, total duration time is the duration between the start and end of all threads, whereas DNS lookup, connection, response, and download time is the sum of the corresponding value of each thread. You can set the required count of URL load threads in the `_urlLoadThreads` property in **<SiteScope root directory>\groups\master.config**.

## Problems Using WinInet

Check the WinInet flow:

- Try to reach your URL in Internet Explorer by opening it in command prompt:  

```
$ runas /user:DOMAIN\USER_NAME "C:\Program Files\Internet Explorer\iexplore.exe /separate"
```

  
where `DOMAIN\USER_NAME` is account of a user under which SiteScope is running,  
If you cannot open the URL, try to analyze why.
- Check for server certificate revocation. If you encounter HTTP Error 12057 (which indicates that revocation cannot be checked because the revocation server is offline), either:
  - Avoid using WinInet, or
  - In Internet Explorer, select **Tools > Internet Options > Advanced > Security**, and switch off **Check for server certificate revocation**.
- Other common problems:
  - Not enough user permissions
  - Cookies are blocked (indicated by a 403 Forbidden error)

## Error Messages

The following error codes might be encountered when working with URL monitors.

Error Code	Description and Troubleshooting
(-982)	Permission denied.
(-983)	SOAP Fault Error.
(-986)	This message is returned when an item is not found in the XML content. Check the XML content by using the <b>View Source</b> command from a browser.
(-987)	This message is returned when a syntax problem is found in the XML content. Check the XML content by using the <b>View Source</b> command from a browser.
(-988)	This message is returned when the value of an item in an XML document is incorrect. Check the XML content by using the <b>View Source</b> command from a browser.

Error Code	Description and Troubleshooting
(-989)	This message is returned when an error string is found in the HTML content. Check the HTML content by using the <b>View Source</b> command from a browser.
(-990)	This message is returned when a link, form, or frame is not found in the HTML on a page. Check the HTML content for that step by using the <b>View Source</b> command from a browser.
(-991)	This message is returned when the server returns an incomplete response. It may be caused by a busy server or network. It may also be caused by a problem in a CGI script. Check the URL using a browser for additional information. Check the load on the network. Check the load on the server.
(-992)	Monitor Specific Error.
(-993)	This message is returned when there is not a network path that reaches the server. Check the network connection to the server. Check that firewalls and routers allow access to the server. Check the load on the network. Check that the server is running.
(-994)	This message is returned when a Windows library has an internal problem. If this problem occurs repeatedly, report it to your system administrator.
(-995)	This message is returned when the content of a URL changes. Check the URL using a browser to view the new contents.
(-996)	This message is returned when a connection is made but not completed. Check the load on the network. Check the load on the server.
(-997)	This message is returned when DNS cannot find an IP address for a name. Check the network connection to the DNS server. Check that the DNS server for that domain is running. Check that DNS is properly configured on the SiteScope machine. Check that the name exists in the configuration for that domain.
(-998)	This message is returned when the server does not accept the connection. Check that the server and server process are running. Check the load on the server. Check the load on the network.
(-999)	This message is returned when the match string is not found in the HTML content. Check the HTML content by using the View Source command from a browser.
(-1000)	URL Unknown Error.
(-1001)	IP address does not match.
(-1002)	Unable to connect to remote monitoring server.

Error Code	Description and Troubleshooting
(-1003)	This message is returned when connection was reset. Check the URL using a browser for additional information. Check the load on the network. Check the load on the server.
(12157)	Insufficient encryption, probably needs 128 bit Internet Explorer.
(12037)	Secure certificate has expired.
(12038)	Secure certificate name does not match host name.
(12044)	Requires client certificate authentication.
(12045)	Certificate authority not registered in SiteScope cacerts file.
(12046)	URL Certificate Peer Error.



# Chapter 106: URL Sequence Monitor

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 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 are not familiar with your application. By using this monitor to perform sequence testing, you can verify that users are able to successfully complete transactions.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **URL Sequence** monitor.

## Learn About

This section includes:

- ["URL Sequence Monitor Overview" below](#)
- ["Working with the URL Sequence Monitor" on the next page](#)
- ["Defining Sequence Steps" on page 699](#)
- ["URL Sequences and Dynamic Content" on page 700](#)
- ["Retaining and Passing Values Between Sequence Steps" on page 702](#)
- ["Sharing Cookies Between Monitor Runs and Configured Monitors" on page 703](#)
- ["Support for IPv6 Addresses" on page 703](#)
- ["SSL Connectivity" on page 704](#)
- ["License Consumption" on page 704](#)

## 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 the SiteScope Dashboard.

## 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. (The default is 20 steps, which you can modify by changing the value of the `_URLSequenceMonitorSteps` property in the `<SiteScope root directory>\groups\master.config` file.) 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. Make sure you are 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 712](#) and Client-side Programs help page.
- 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.

## 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.
Following a Hyperlink	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.
Selecting a Form button	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.  The listings are in the following format: {[formNumber]}FormName}ButtonName  <b>Example:</b> The Search button on a company's search page might be listed as: {[1]http://www.CompanyName.com/bin/search}search
Selecting a Frame within a frameset	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.
Following a META REFRESH redirection	If the page for this step of the sequence is controlled by a <META HTTP-EQUIV="Refresh" CONTENT="timedelay; URL=filename.htm"> 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.

**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.

## 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

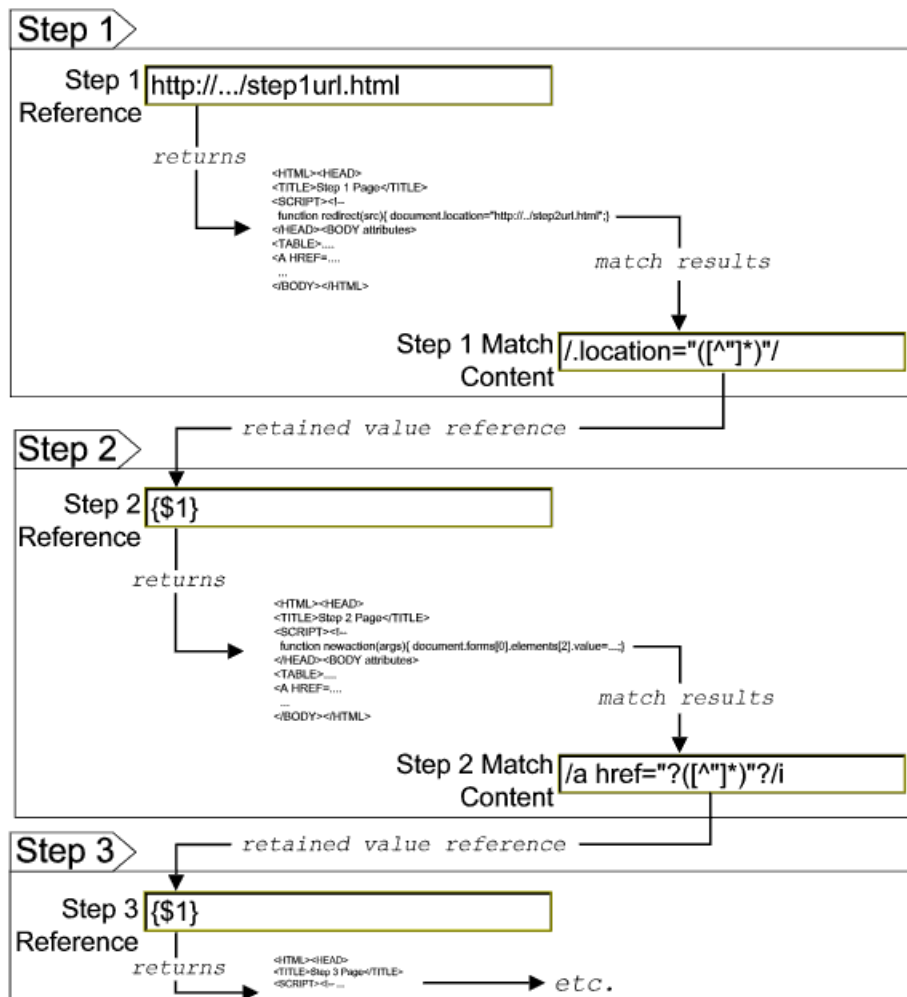
There are several ways to make a SiteScope URL Sequence monitor perform actions controlled by client-side programs and other dynamic content. Several of these workarounds are presented below. The workarounds generally require knowledge of the principles of Web page construction, CGI programming, Perl-style Regular Expressions Overview, and the programming used to support the Web site being monitored.

Dynamic Content	SiteScope Workaround
A Web page contains a script which controls a link to another URL. <b>Example:</b> <code>onClick = "document.location='http://..."</code>	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.
A client-side program reformats, edits, or adds data to a POST or GET data set collected by HTML form inputs.	Manually edit the script changes into the NAME=VALUE 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.
A client-side program generates HTML content which, after interpretation by a Web browser, includes HTML <code>&lt;A HREF=...&gt;</code> links.	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.

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 <b>NAME=VALUE</b> 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 <b>ACTION</b> attribute of an HTML <b>&lt;FORM&gt;</b> tag.	Manually enter the <b>ACTION</b> 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 <b>METHOD</b> attribute of an HTML <b>&lt;FORM&gt;</b> tag.	Manually enter the <b>POST</b> or <b>GET</b> data for the next sequence step. For <b>POST</b> methods, enter the data in the <b>POST data</b> box in the HTTP Settings section of the URL Sequence Step dialog box. For <b>GET</b> methods, enter the <b>ACTION</b> URL plus the <b>&amp;NAME=VALUE</b> 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 **\$nth** 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)[\V-\=]*?(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 on' 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.

## Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP and HTTPS protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("`[`", "`]`"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## 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 Sequence Monitor" on page 697](#).
- Importing the server certificate. For details on how to perform this task, see ["How to Configure the URL Sequence Monitor" below](#).

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol/HTTP Client used by SiteScope	Java ("Use WinInet" is not selected)	WinInet ("Use WinInet" is selected)
SSLv2	x	x
SSLv3	√	√
TLSv1.0, TLSv1.1, TLSv1.2	√	√

## License Consumption

Points-based Usage	Capacity-based Usage
One point per URL (Step)	One URL license per monitored URL

## Tasks

This section includes:

- ["How to Configure the URL Sequence Monitor" below](#)
- ["How to Manually Import Server Certificates" on page 706](#)

## How to Configure the URL Sequence Monitor

### 1. Prerequisites

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.

### 2. 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 [How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide](#).



- Import the server certificates manually. For details, see ["How to Manually Import Server Certificates" on the next page.](#)

### 3. 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 in the Using SiteScope Guide.

### 4. 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. Configure 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 the collected data. For details on the URL Sequence test, see ["URL Sequence Steps Results Dialog Box" on page 715.](#)

For details on the URL Sequence Step dialog box, see ["URL Sequence Step Dialog Box" on page 707.](#)

### 5. 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 699.](#)

- c. Configure the other sequence step settings as necessary and click **OK**. For user interface details, see ["URL Sequence Step Dialog Box" on page 707.](#)

### 6. 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:	<div>[[2]signInForm)email= [[2]signInForm)newCustomer=registeredCusto mer [[2]signInForm)password=mypassword</div>
Post Data Password Key:	<input type="text"/>
Post Data Password Value:	<input type="text"/>

**Example - Encrypted Password:**

POST data:	<div>[[2]signInForm)email= [[2]signInForm)newCustomer=registeredCusto mer [[2]signInForm)password=</div>
Post Data Password Key:	<input type="text" value="password"/>
Post Data Password Value:	<input type="text" value="*****"/>

## 7. Configure other settings for the monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

## How to Manually Import Server Certificates

Instead of using Certificate Management, you can manually import certificates 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 in the Using SiteScope Guide.

1. Check the certificates already in the keystore, from the **<SiteScope root directory>\javallib\security** directory, by entering:

```
../..bin/keytool -list -keystore cacerts
```

2. Import the certificate, into **<SiteScope root directory>\javallib\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.







## UI Descriptions

This section includes:

- ["Step Settings" below](#)
- ["URL Sequence Step Dialog Box" below](#)
- ["URL Sequence Monitor Settings" on page 712](#)
- ["URL Sequence Steps Results Dialog Box" on page 715](#)

### Step Settings

User interface elements are described below:

UI Element	Description
	<b>New Step.</b> Opens the URL Sequence Step dialog box enabling you to define the URL sequence steps. For user interface details, see <a href="#">"URL Sequence Step Dialog Box" below</a> .
	<b>Edit Step.</b> Opens the URL Sequence Step dialog box enabling you to edit the properties of an existing URL sequence step. For user interface details, see <a href="#">"URL Sequence Step Dialog Box" below</a> .
	<b>Delete Last Step.</b> Deletes the last step in the URL sequence.
	<b>Select All.</b> Selects all listed URL sequence steps.
	<b>Clear Selection.</b> Clears the selection.
	<b>Test Steps.</b> Runs the defined steps in the URL Sequence, and display the results of the collected data. The response embeds a copy of the HTML received from the HTTP request. For details, see <a href="#">"URL Sequence Steps Results Dialog Box" on page 715</a> .
<b>Step</b>	The step number in the URL sequence.
<b>Reference Type</b>	URL of the sequence step.
<b>Title</b>	Name of this step within the sequence monitor.

### URL Sequence Step Dialog Box

This dialog box 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 **User name** and **Password** settings are only sent as part of

the request being made in the step that they are defined.

**To access:** Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **URL Sequence** monitor. In the **Step Settings** panel, click the **New Step** or **Edit Step** button.

User interface elements are described below:

UI Element	Description
<b>Reference Settings</b>	
<b>&lt;Reference type&gt;</b>	<p>Use these options to select how SiteScope progresses from one step of a URL sequence to the next. For details, see <a href="#">"Defining Sequence Steps" on page 699</a>.</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. This is the only option available as the starting point for the sequence (step 1).</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 <a href="#">"URL Sequences and Dynamic Content" on page 700</a>.</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.

UI Element	Description
<b>Match content</b>	<p>Text string to match in the returned page or frameset. If the text is not contained in the page, the monitor displays the message <b>content match error</b>. The search is case sensitive.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>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. For example, <code>&lt; B&gt; Hello&lt; /B&gt; World</code>.</li> <li>You can also perform a regular expression match by enclosing the string in forward slashes, with a letter <code>i</code> after the trailing slash indicating case-insensitive matching. For example, <code>/href=Doc\d+\.html/</code> or <code>/href=doc\d+\.html/i</code>.</li> <li>You can search for a pattern string across multiple lines. To do so, add the <code>/s</code> modifier to the end of the regular expression. For example, <code>/(state).*(populate)/s</code> checks if the returned page contains both "state" and "populate".</li> </ul> <p>For details on regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.</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>
<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>

UI 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> (default value). Select to have SiteScope use the settings specified in the <b>Pre-emptive authorization</b> field in the General Settings 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.</li> </ul> <p><b>Note:</b> If the URL does not require a user name and password, this option may cause the URL to fail.</p> <ul style="list-style-type: none"> <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.</li> </ul> <p><b>Note:</b> If the URL does not require a user name and password, this option may be used.</p> <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 General Settings 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>&lt;SiteScope root&gt;\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>
<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 Windows NT LAN Manager (NTLM) authorization if it is required to access the URL in this step.</p>
<b>HTTP Settings</b>	
<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>

UI Element	Description
<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.
<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, <code>gmail.com</code> sends. The site <code>gmail.com</code> 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 <code>gmail.com</code> is <code>Passwd</code>. 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 <a href="#">"How to Configure the URL Sequence Monitor" on page 704</a>.</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>	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.
<b>Show HTML</b>	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.

## URL Sequence Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, to 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>Uses the value entered for the <b>Timeout</b> 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>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>Specifies 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>
<b>Show detailed measurements</b>	<p>SiteScope records 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>	



UI Element	Description
<b>Request headers</b>	<p>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>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>
<b>Retrieve images</b>	<p>Status and response time statistics 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>SiteScope retrieves the frames references in a frameset and counts 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>
<b>Use WinInet</b>	<p>WinInet is used as an alternative HTTP client for this monitor.</p> <p>Select this option to use WinInet instead of Java (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 such as SSLv3, 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> <p><b>Note:</b> WinInet functionality is available on Windows versions of SiteScope only. For troubleshooting WinInet functionality, see <a href="#">"Problems Using WinInet" on page 717</a>.</p>
<b>Proxy Settings</b>	


UI Element	Description
<b>HTTP proxy</b>	Domain name and port of an HTTP Proxy Server if a proxy server is used to access the URLs in the sequence.
<b>Proxy server user name</b>	Proxy server user name if required to access the URLs in the sequence. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	Proxy server password if required to access the URLs in the sequence. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy NTLM V2</b>	Select if the proxy server requires authentication using NTLM version 2.
<b>Authentication Settings</b>	
<b>NTLM V2</b>	Select if the URL you are accessing requires authentication using NTLM version 2. <b>Default value:</b> Not selected
<b>Preferred protocols</b>	<p>Select the preferred protocol option to use for the handshake process.</p> <ul style="list-style-type: none"> <li>• <b>Any supported protocol.</b> Enables any supported protocol to be used for the handshake process (this is the default setting). Since this option uses SSL protocols, SSL must be enabled on the Web server to use this option.</li> <li>• <b>Prefer SSL to TLS.</b> Select if the URL you are accessing cannot handle authentication using TLS. This enables encrypted handshake messages to be sent using SSL. <b>Note:</b> This option is ignored (if selected) when SiteScope is running in FIPS 140-2 mode, since authentication using TLS is mandatory with FIPS 140-2. For details on FIPS 140-2, see the Running SiteScope Securely section of the SiteScope Deployment Guide (&lt;SiteScope root directory&gt;\sisdocs\doc_lib\Get_Documentation.htm).</li> <li>• <b>Prefer TLS to SSL.</b> Select if you prefer to use TLS for encrypting handshake messages or if the URL you are accessing cannot handle authentication using SSL. TLS is the latest cryptographic protocol. TLS 1.0, 1.1, and 1.2 are supported.</li> <li>• <b>Prefer TLSv1.0.</b> Select if you prefer to use only the TLS 1.0 version.</li> <li>• <b>Prefer TLSv1.1.</b> Select if you prefer to use only the TLS 1.1 version.</li> <li>• <b>Prefer TLSv1.2.</b> Select if you prefer to use only the TLS 1.2 version.</li> </ul>
<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 <a href="#">"SSL Connectivity" on page 704</a>.</p> <p><b>Default value:</b> Not selected</p>

UI Element	Description
<b>Accept invalid certificates for HTTPS</b>	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. <b>Default value:</b> Not selected
<b>Use cookie persistency</b>	Shares cookies between monitor runs and between configured monitors. For details, see <a href="#">"Sharing Cookies Between Monitor Runs and Configured Monitors" on page 703</a> . <b>Default value:</b> Not selected
<b>Load cookies from persistency</b>	Loads all relevant cookies from the persistency file and adds them to the list of cookies to be sent to the server. Cookies are loaded at the beginning of the monitor run. <b>Default value:</b> Not selected
<b>Save cookies to persistency</b>	Saves 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. <b>Default value:</b> Not selected
<b>Cookie persistency file path</b>	Path and name of the cookie persistency file.

## URL Sequence Steps Results Dialog Box

This dialog box displays the collected data from running all the URL steps defined in the Step Settings panel. This includes the status of the overall sequence, the response time for each step and the content match for each step in the sequence (if applicable). 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.

### To access:

1. Select the **Monitors** context.
2. In the monitor tree, right-click a group, select **New > Monitor**, and select the **URL Sequence** monitor.
3. In the **Step Settings** panel, configure the individual steps for the URL sequence, and then click the **Test Steps**  button to view the test results.
4. In the URL Sequence Steps Results dialog box, use the step hyperlinks at the top to navigate to any step in the sequence.

User interface elements are described below:

UI Element	Description
<b>&lt;Step # link&gt;</b>	Links to the relevant step in the results.

UI Element	Description
Save to file	Opens the Save dialog box, enabling you to save the sequence steps results to an HTML file.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

- Certificate Expiration Days Remaining - Number of days to the earliest expiration date of any certificate in the chain of certificate that was used to establish the SSL connection.
- content match - Displays the text string to match in the returned page or frameset.
- round trip time (milliseconds) - Amount of time to complete the following: (1). Name lookup, DNS (2). Connect to the server socket (3). Send the HTTP request (4). Download the entire page. While this counter is measured in milliseconds in the Threshold Settings, it is displayed in seconds in the SiteScope Dashboard.
- status - Relates only to HTTP status codes (such as 200, 302, and 404) in the page itself.
- <step title> connect time (for steps 1-10)
- <step title> dns time (for steps 1-10)
- <step title> download time (for steps 1-10)
- <step title> response time (for steps 1-10)
- <step title> round trip time (for steps 1-10)
- total errors - The total number of errors encountered downloading the page.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and limitations:

- ["General Notes/Limitations" below](#)
- ["Problems Using WinInet" on the next page](#)
- ["Error Messages" on the next page](#)

### General Notes/Limitations

- You can run all the steps defined in the URL sequence by clicking the **Test Steps** button in the Step Settings panel or the **Tools** button in the SiteScope Dashboard. This displays the collected data from each step, and embeds a copy of the HTML page returned. For details, see ["Step Settings" on page 707](#).
- If a step fails, an error message is displayed and the sequence steps report is not generated.
- When using several URL load threads, the total duration time might be less than the combined total of the DNS lookup, connection, server response, and download time. In this case, total duration time is the duration between the start and end of all threads, whereas DNS lookup, connection, response, and download time is the sum of the corresponding value of each thread. You can set the required count of URL load threads in the `_urlLoadThreads` property in **<SiteScope root**

#### **directory>\groups\master.config.**

- The "Certificate Expiration Days Remaining" counter shows the minimum number of days remaining for the different certificates used in steps, or shows 0 if no step uses a secured connection.
- Step title was missing from URL sequence reports in SiteScope versions earlier than 11.23 (instead, there was step number). After upgrading an earlier version of SiteScope that contained URL Sequence monitors:
  - Changes in URL sequence counter names are shown in the Dashboard.
  - URL sequence report shows the following changes:
    - Reports that contain monitor runs from before and after the upgrade show the same metric with two different names.
    - Reports that only contain monitor runs from after the upgrade show the updated metric names (with <step title>).
    - Reports that only contain monitor runs from before the upgrade show the old metric names (without the <title> part).

## **Problems Using WinInet**

Check the WinInet flow:

- Try to reach your URL in Internet Explorer by opening it in command prompt:  

```
$ runas /user:DOMAIN\USER_NAME "C:\Program Files\Internet Explorer\iexplore.exe /separate"
```

where DOMAIN\USER\_NAME is account of a user under which SiteScope is running,  
If you cannot open the URL, try to analyze why.
- Check for server certificate revocation. If you encounter HTTP Error 12057 (which indicates that revocation cannot be checked because the revocation server is offline), either:
  - Avoid using WinInet, or
  - In Internet Explorer, select **Tools > Internet Options > Advanced > Security**, and switch off **Check for server certificate revocation**.
- Other common problems:
  - Not enough user permissions
  - Cookies are blocked (indicated by a 403 Forbidden error)

## **Error Messages**

The following error codes might be encountered when working with URL monitors.

<b>Error Code</b>	<b>Description and Troubleshooting</b>
(-982)	Permission denied.
(-983)	SOAP Fault Error.

Error Code	Description and Troubleshooting
(-986)	This message is returned when an item is not found in the XML content. Check the XML content by using the <b>View Source</b> command from a browser.
(-987)	This message is returned when a syntax problem is found in the XML content. Check the XML content by using the <b>View Source</b> command from a browser.
(-988)	This message is returned when the value of an item in an XML document is incorrect. Check the XML content by using the <b>View Source</b> command from a browser.
(-989)	This message is returned when an error string is found in the HTML content. Check the HTML content by using the <b>View Source</b> command from a browser.
(-990)	This message is returned when a link, form, or frame is not found in the HTML on a page. Check the HTML content for that step by using the <b>View Source</b> command from a browser.
(-991)	This message is returned when the server returns an incomplete response. It may be caused by a busy server or network. It may also be caused by a problem in a CGI script. Check the URL using a browser for additional information. Check the load on the network. Check the load on the server.
(-992)	Monitor Specific Error.
(-993)	This message is returned when there is not a network path that reaches the server. Check the network connection to the server. Check that firewalls and routers allow access to the server. Check the load on the network. Check that the server is running.
(-994)	This message is returned when a Windows library has an internal problem. If this problem occurs repeatedly, report it to your system administrator.
(-995)	This message is returned when the content of a URL changes. Check the URL using a browser to view the new contents.
(-996)	This message is returned when a connection is made but not completed. Check the load on the network. Check the load on the server.
(-997)	This message is returned when DNS cannot find an IP address for a name. Check the network connection to the DNS server. Check that the DNS server for that domain is running. Check that DNS is properly configured on the SiteScope machine. Check that the name exists in the configuration for that domain.
(-998)	This message is returned when the server does not accept the connection. Check that the server and server process are running. Check the load on the server. Check the load on the network.

Error Code	Description and Troubleshooting
(-999)	This message is returned when the match string is not found in the HTML content. Check the HTML content by using the View Source command from a browser.
(-1000)	URL Unknown Error.
(-1001)	IP address does not match.
(-1002)	Unable to connect to remote monitoring server.
(-1003)	This message is returned when connection was reset. Check the URL using a browser for additional information. Check the load on the network. Check the load on the server.
(12157)	Insufficient encryption, probably needs 128 bit Internet Explorer.
(12037)	Secure certificate has expired.
(12038)	Secure certificate name does not match host name.
(12044)	Requires client certificate authentication.
(12045)	Certificate authority not registered in SiteScope cacerts file.
(12046)	URL Certificate Peer Error.

# Chapter 107: VMware Datastore Monitor

Use the VMware Datastore monitor to monitor the state of VMware Datastores and Virtual Disks (connectivity, capacity, free space, and snapshot size).

**Tip:** SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of VMware monitoring. For details, see VMware Capacity Management Solution Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the **VMware Datastore** monitor.

## Learn About

This section includes:

- ["VMware Datastore Monitor Overview" below](#)
- ["Supported Platforms/Versions" on the next page](#)
- ["SSL Connectivity" on the next page](#)
- ["Connection Pool Settings" on the next page](#)
- ["VMware Datastore Monitor Topology" on the next page](#)
- ["System Tuning for Loaded Environments" on page 722](#)
- ["License Consumption" on page 723](#)

## VMware Datastore Monitor Overview

SiteScope simplifies the monitoring of virtual storages changes in dynamic, virtualized environments by automatically changing the SiteScope configuration according to changes in the virtual environment. The VMware Datastore monitor is dynamically updated over time by adding or removing counters as datastores and virtual disks are added or removed from the VMware Datacenters. This enables you to configure the monitor once, and leave it to automatically discover changes in the environment and update itself.

During initial monitor creation, the monitor uses the connection URL configured to access the VMware datacenters in the vCenter and dynamically discover the exists datastores and virtual disks. You can select from these performance counters to determine which measurements SiteScope should retrieve for reporting datastore status.

You can also define the required thresholds for the counter's pattern. In this way, thresholds are also updated automatically when the counters are updated.

For details describing all the available counters, refer to the VMware documentation available at <http://www.vmware.com/support/developer/vc-sdk/visdk25pubs/ReferenceGuide/>.

For details on the dynamic monitoring mechanism, see Dynamic Monitoring Mechanism in the Using SiteScope Guide.



## Supported Platforms/Versions

This monitor supports monitoring remote servers running on VMware vSphere 4.0, 4.1, 5.0, 5.1, 5.5, 6.0.

## 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 ["How to import the VMware Server Certificates" on page 725](#).

## Connection Pool Settings

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. The connection pool is a set of pools per key. A key is the combination of a vCenter, and a user (the connection cannot be shared between different users due to different permissions)

If all VM monitors are configured with the same vCenter URL and user, one connection pool is created. For two vCenters and two different users for every vCenter, four connection pools are created.

The connection pool configures itself over time to ensure that only active connections stay in the pool. It does this by running an additional thread at the rate of the connection timeout multiplied by two; if the connection timeout is 30 minutes, it will run once every hour and evict idle connections from the pool. Connections that are idle for more than half a minute before the connection timeout are eligible for eviction.

For example, if the connection timeout is 30 minutes, the thread will evict connections that were idle for more than 29.5 minutes, but less than 30 minutes (to avoid a connection timeout). The connections that were idle more than 30 minutes are evicted by the timeout process. As a result, only active connections stay in the pool.

You can configure the following connection pool properties in **Preferences > Infrastructure Preferences > Custom Settings**:

- **VMware maximum idle connections in pool.** The maximum number of idle connections in the pool. The default value is 60.
- **VMware connection active connections in pool.** The maximum number of active connections in the pool. The default value is 60.

**Note:** If a SiteScope is registered to BSM, it uses more connections to retrieve properties relevant for topology reporting. Therefore, you should increase the maximum number of idle and active connection properties to enable SiteScope to perform well.

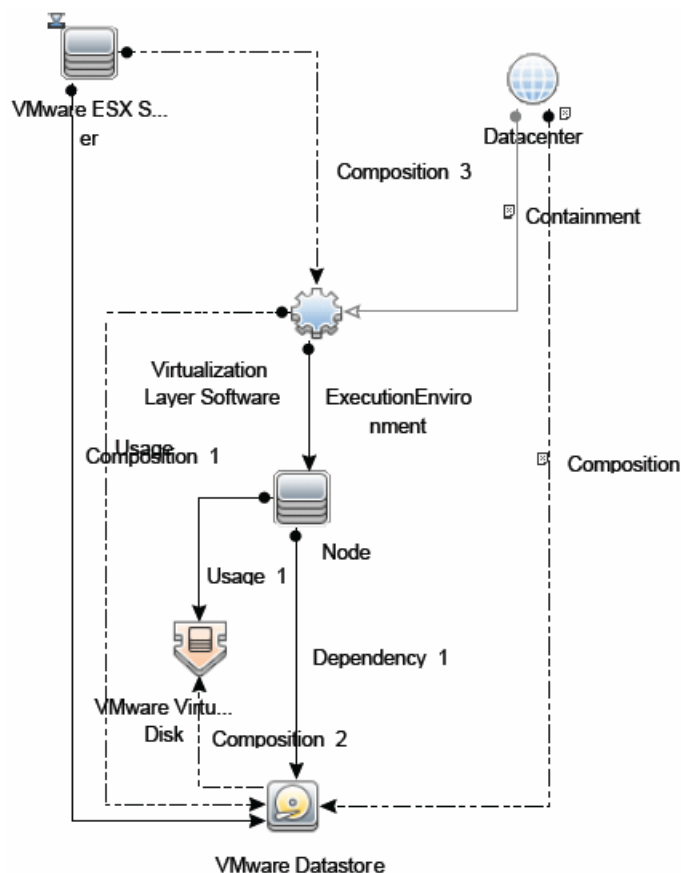
- **VMware connection timeout (minutes).** Connection timeout in minutes. The default value is 30 minutes.

**Tip:** We recommend setting the maximum size of total connections to the number of configured VM monitors in SiteScope, and let the internal connection pool mechanism optimize itself.

## VMware Datastore Monitor Topology

**Note:** Topology reporting is supported for this monitor when SiteScope is connected to BSM 9.20 or later.

The VMware Datastore monitor can identify the topology of the VMware servers being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

## System Tuning for Loaded Environments

SiteScope installed on a 64-bit environment supports configurations with up to 2000 VMware datastore monitors running concurrently. This loaded system can be integrated with BSM and OM metrics.

To support loaded environments, the following system tuning is required:

- SiteScope sizing is required to increase JVM heap size, desktop heap size, and the number of file handles. You can use the SiteScope Configuration Tool to size SiteScope. For details, see Using the SiteScope Configuration Tool in the SiteScope Deployment Guide (<SiteScope root directory>\sdocs\doc\_lib\Get\_Documentation.htm).
- Add the **\_runGCPeriod=1200000** property to the **<SiteScope root directory>\groups\master.config** file. This means that SiteScope initiates running the garbage collector every 20 minutes (1200000 milliseconds) for better performance.
- Tune the following vCenter connections parameters in **Preferences > Infrastructure Preferences > Custom Settings**, as required:
  - **VMware maximum idle connections in pool**
  - **VMware connection active connections in pool**

- **VMware connection timeout (minutes)**
- Increase the number of dynamic monitors handles in **Preferences > Infrastructure Preferences > Dynamic Monitoring Settings**:
  - **Dynamic monitoring core thread pool size**: 50
  - **Dynamic monitoring maximum thread pool size**: 70

## License Consumption

Points-based Usage	Capacity-based Usage
One point per datastore	One OS instance per datastore. As a result, OSi capacity consumption for Dynamic VMware monitors can change during the monitor run according to the number of discovered datastores.  Note: Monitor is not available when using Community edition.

## Tasks

This section includes:

- ["How to Configure the VMware Datastore Monitor" below](#)
- ["How to import the VMware Server Certificates" on page 725](#)

## How to Configure the VMware Datastore Monitor

### 1. Prerequisites


- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- The monitored vCenter server must be directly accessible by the SiteScope server (no proxy involved).
- The vCenter server provides connection either by http or by https (depending on the vCenter server configuration). If https is used, server certificate must be imported to the SiteScope. For task details, see ["How to import the VMware Server Certificates" on page 725](#).

### 2. Configure the monitor properties

For each VMware Datastore monitor, you can:

- Create the monitor by deploying the VMware Capacity Management solution template (recommended). The template contains a predefined monitor set with optimized settings that allow you to monitor only the relevant components. For solution template details, see VMware Capacity Management Solution Templates in the Using SiteScope Guide.
- Create the monitor manually (as described in How to Deploy a Monitor in the Using SiteScope Guide), and then configure the settings as specified below.

**To create the monitor manually:**

- a. Right-click the group into which you want to add the monitor instance, select **New > Monitor**, and select **VMware Database**. The New VMware Database Monitor dialog box opens.
- b. Click the **Get Counter** button, and select the counters you want to monitor from the Select Counters Form. The counters are added to the Preview tree in the **Patterns & Counters** section.
- c. For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
  - Clicking the **Add New Counter**  button to add an empty line to the table, and creating a pattern format using a regular expression.

**Tip:**


- (1). The pattern should always start and end with the forward slash ("/") character.
- (2). The "[" and "]" characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character).
- (3). Use "." to describe any character any number of times.

For example, if you enter the pattern `./././accessible/`, the monitor retrieves the accessible counter for all datastores .

- Selecting a static counter, and editing the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.

**Example:**

If you enter the pattern `./././accessible/`, the monitor retrieves the `accessible` counter for all datastores.

- d. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counter Preview tree.
- e. Set the frequency for updating counters from the server in the **Frequency of updating counters from server** box. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- f. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful for keeping track of the counters that were previously being monitored.
- g. Click **Verify & Save** or **Save** to save your settings.
- h. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

### 3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting).

For user interface details, see BSM Integration Data and Topology Settings in the Using SiteScope Guide.

#### 4. Configure the connection pool mechanism - optional

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. We recommend setting the maximum size of total connections (in **Preferences > Infrastructure Preferences > Custom Settings > VMware connection active connections in pool**) to the number of configured VM monitors in SiteScope, and letting the internal connection pool mechanism optimize itself.

For details, see ["Connection Pool Settings" on page 721](#).

#### 5. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the vCenter service and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:

- The SiteScope **Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.

For additional troubleshooting suggestions, see ["Tips/Troubleshooting" on page 728](#).

### How to 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 either:

- Using Certificate Management in the SiteScope Preferences. For task details, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
- Manually using the keytool method (see procedure below for details).

#### 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, 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.

## UI Descriptions

### VMware Datastore Monitor Settings

User interface elements are described below:

UI Element	Description
<b>URL</b>	<p>URL of the VMware vCenter on the datastores that 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 datastore server. You can import the server certificates directly from the monitor using SiteScope's Certificate Management (click the <b>Import Certificates</b> icon), instead of importing certificates manually.</p> <p><b>Note:</b> If you get 'Error Code: 31008. Error getting counters' when SSL is used, navigate to <b>Preferences &gt; Infrastructure Preferences &gt; General Settings</b>, and select <b>Accept untrusted SSL certificates</b>.</p>
<b>Credentials</b>	<p>User name and password required to access the VMware datastore. 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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>VM Disk Timeout (seconds)</b>	<p>Amount of time, in seconds, to wait for the datastore to find its virtual disks before timing out.</p> <p><b>Default value:</b> 1</p>

UI Element	Description
<b>Patterns &amp; Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Click the <b>Add New Counter</b>  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the <b>Delete Counter</b>  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the <b>View Matches for Selected Pattern Counter</b>  button to display counters that match the selected patterns.</p> <p><b>Note:</b> SiteScope uses Perl regular expressions for pattern matching. Accordingly, you should use Perl regular expressions to specify patterns for VMware Datastore monitor counters. For example, if you enter <code>/cpu.*/</code> or <code>cpu</code>, any counters with <code>cpu</code> in their name match this pattern and are added to the counters list.</p>
<b>Get Counters</b>	<p>Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.</p> <p>You can configure the following counters for this monitor:</p> <ul style="list-style-type: none"> <li>• <b>Datastore:</b> name , accessible , capacity, freeSpace, freeSpace in %, url, snapshots size</li> <li>• <b>Virtual Disk snapshot:</b> capacity, path</li> <li>• <b>Virtual Disk:</b> capacity, path, type, usage</li> </ul>
<b>Counter Preview</b>	<p>Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.</p>
<b>Frequency of updating counters from server</b>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p><b>Default value:</b> 15 minutes</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The update frequency cannot be less than the monitor run frequency in Monitor Run Settings.</li> <li>• When configuring this setting in a template, the variable value can only be in time units of seconds.</li> <li>• Static counters are never deleted.</li> </ul>

UI Element	Description
<b>Continue displaying counters that no longer exist after update</b>	<p>Counters that no longer exist after running the update mechanism to retrieve counters from the VMware server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful if a server goes down or for keeping track of what counters were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings.</p> <p><b>Default value:</b> Selected</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

This section describes troubleshooting and limitations for the VMware Datastore monitor.

- ["General Notes" below](#)
- ["Maximum Number of Counters That Can be Saved" below](#)
- ["DNS Reconciliation Issues When Monitoring VMware-based Servers" on the next page](#)
- ["Troubleshooting Logs" on the next page](#)

### General Notes

- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).

### Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the **\_browsableContentMaxCounters** parameter in the **master.config** file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the **\_maxCountersForRegexMatch** parameter in the **master.config** file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The **\_maxCountersForRegexMatch** parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same



value for both **\_browsableContentMaxCounters** and **\_maxCountersForRegexMatch** parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

## DNS Reconciliation Issues When Monitoring VMware-based Servers

SiteScope performs DNS resolution to resolve new target hosts. When monitoring VMware-based servers, instead of using the DNS resolution mechanism, SiteScope resolves DNS using the VMware vCenter.

**Problem:** In some cases, there might be reconciliation issues. For example, when creating a new VM by cloning or deploying from a template, the new VM can be initialized with its parent VM\template DNS name.

However, for topology to be reported correctly, each VM name must represent its DNS name (the VM name must contain its short DNS name).

### Example:

```
VM1:
VM name: VMSiteScope1
DNS name: VMSiteScope1.hp.com

VM2:
VM name: VMSiteScope2
DNS name: VMSiteScope2Clone.hp.com
```

**Solution:** To enable correct topology reporting, you must set the **\_shouldCheckIfVmDNSConfigured** property to **=true** in the **<SiteScope home>\groups\master.config** file.

## Troubleshooting Logs

1. Check for dynamic framework errors in:

- **<SiteScope root directory>\logs\dynamic\_monitoring\_changes.log**. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
- **<SiteScope root directory>\logs\dynamic\_monitoring.log**. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).

To check for dynamic monitoring errors, copy the following section from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
#####
# Dynamic Monitoring
#####
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=false
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFileAppender
log4j.appender.dynamic.monitoring.appender.File=../${log.file.path}/dynamic_monitoring.log
```

```
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
```

2. Check for VMware monitor errors in:

- **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.
- **<SiteScope root directory>\logs\vmware\_connections.log**. This log provides information about the connection pool against the ESX/vCenter (get/return connection).

To view VMware monitor errors, copy the following sections from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
# VMware Connection Pool
#####
log4j.category.VMwareConnectionPool=${monitor.loglevel}, vmware.connection.pool.appender
log4j.additivity.VMwareConnectionPool=false
log4j.appender.vmware.connection.pool.appender=org.apache.log4j.RollingFileAppender
log4j.appender.vmware.connection.pool.appender.File=../${log.file.path}/vmware_connections.log
log4j.appender.vmware.connection.pool.appender.MaxFileSize=${def.file.max.size}
log4j.appender.vmware.connection.pool.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.vmware.connection.pool.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.vmware.connection.pool.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
```

# Chapter 108: VMware Host Monitors

Enables you to monitor CPU, memory, network, state and storage-related counters of the VMware host server and its guest virtual machines, as described in "[VMware Host Monitor Overview](#)" below.

## Tip:

- SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of VMware monitoring. For details, see VMware Host Solution Template in the Using SiteScope Guide.
- You can view a guided and narrated demonstration for the VMware Host monitors on YouTube: <http://www.youtube.com/watch?v=A7Tzb-lb168&feature=plcp>.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the required VMware Host monitor.

## Learn About

This section includes:

- "[VMware Host Monitor Overview](#)" below
- "[Supported Versions/Platforms](#)" on the next page
- "[VMware Performance Monitor or VMware Host Monitor?](#)" on page 733
- "[Smart Counters](#)" on page 733
- "[SSL Connectivity](#)" on page 734
- "[Connection Pool Settings](#)" on page 734
- "[VMotion Support](#)" on page 735
- "[VMware Host Monitors](#)" above
- "[System Tuning for Loaded Environments](#)" on page 737
- "[Metrics Integration Support](#)" on page 737
- "[License Consumption](#)" on page 738

## VMware Host Monitor Overview

Virtualization is one of the most important technologies in IT infrastructures that creates new complexities when it comes to managing the virtualization environment. Virtual Machines (VMs) and their host VMware ESX Servers need performance and availability monitoring.

SiteScope simplifies the monitoring of virtual infrastructure changes in dynamic, virtualized environments by automatically changing the SiteScope configuration according to changes in the virtual environment. VMware Host monitors are dynamically updated over time by adding or removing counters as virtual machines are added or removed from the VMware Host. This enables you to configure the monitor one time, and leave it to automatically discover changes in the environment and update itself. The update is not only as a result of

VMotion, but also when a new CPU, disk, or other resource is added or removed from the host server or guest VM.

Use the VMware Host monitors to monitor performance related resources (CPU, memory, network, state, and storage) on the host server and its guest VMs. The VMware Host CPU and VMware Host Memory monitors also include "smart" configuration counters that provide resource optimization recommendations to help you analyze and solve problems in dynamic virtual infrastructures and maximize resource usage. For details, see ["Smart Counters" on the next page](#).

During initial monitor creation, the monitors use the connection URL configured to access the vCenter or physical host URL 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.

You can also define the required thresholds for the counter's pattern. In this way, thresholds are also updated automatically when the counters are updated.

For details describing all the available counters, refer to the VMware documentation available at <http://www.vmware.com/support/developer/vc-sdk/visdk25pubs/ReferenceGuide/>.

For details on the dynamic monitoring mechanism, see Dynamic Monitoring Mechanism in the Using SiteScope Guide.

**Tip:** We recommend adding VMware Host monitors by deploying the VMware Host solution template instead of creating the monitors manually. The template has a predefined monitor set with optimized settings based on VMware best practices for troubleshooting the ESX/Host server; it monitors only the relevant components (counter patterns) in dynamic environments, and provides the minimum data required for troubleshooting problems in the monitored infrastructure. For details, see VMware Capacity Management Solution Templates in the Using SiteScope Guide.

## Supported Versions/Platforms

This monitor supports monitoring remote servers running on:

- VMware VirtualCenter 2.x
- VMware ESX 3.x, 4.0, 4.1
- VMware ESXi 3.5, 4.0, 4.1, 5.0, 5.1, 5.5, 6.0
- VMware ESX 2.5 via VirtualCenter 2.x
- VMware ESX 3.x via VirtualCenter 3.x
- VMware vSphere 4.0, 4.1, 5.0, 5.1 (also supported with SSO login), 5.5, 6.0

**Note:** Monitoring VMware ESX(i) is not supported when Lockdown mode is enabled.

## VMware Performance Monitor or VMware Host Monitor?

	VMware Performance Monitor	VMware Host Monitors
<b>Type of user</b>	VM user/owner  <b>Note:</b> For vCenter Server 5.1 and 5.5, you can use a user with "Read-only" role.	Virtualization administrator  <b>Note:</b> For vCenter Server 5.1 and 5.5, you can use a user with "Read-only" role.
<b>Requirements</b>	<ul style="list-style-type: none"> <li>Measure performance and availability of a particular VM or set of VMs.</li> <li>Display SiteScope and BSM reports and BSM topology for this VM.</li> </ul> <p>Usually, VM users/owners are not interested on which host the VM runs or other issues.</p>	<ul style="list-style-type: none"> <li>Manage a virtualization environment or vCenter and provide VM services to other users.</li> <li>Measure the availability and performance of vCenter resources (physical host machines).</li> </ul> <p>Usually, virtualization administrators are not interested in specific VMs (only if this machine causes performance issues to the host).</p>
<b>Recommended Use</b>	Monitoring one or a set of VMs	Deploy using VM Host solution template
<b>Benefits</b>	Measures the data every monitor run regardless of whether the VM has migrated.	<ul style="list-style-type: none"> <li>Enables the administrator to make most efficient use of host resources (create maximum VMs and serve more users).</li> <li>Provides notifications of availability and performance problems on the host (that might be caused by specific VM or VMs).</li> <li>The monitor is dynamically updated (see <a href="#">"VMware Host Monitors" on page 731</a>).</li> <li>Smart counters provide useful information for configuring the VM on the host to help maximize resource usage. For details, see <a href="#">"Smart Counters" below</a>.</li> </ul>
<b>Data in SiteScope and BSM Reports</b>	Provides user with SiteScope and BSM reports with continuous data and topology that match the changes (the same VM connects to the relevant host).	<ul style="list-style-type: none"> <li>Enables the administrator to check host information only (the data is continuous). The topology matches VM migration for the monitored hosts.</li> <li>Does not provide continuous data on the VM (every time a VM migrates from host to host, its ID changes in SiteScope and BSM reports). However, VM data does not interest the administrator.</li> </ul>

## Smart Counters

The VMware Host CPU and VMware Host Memory monitors also have a set of smart counters that provide information on the configured resources and the resources that are actually used. This information helps you

to use host resources more efficiently by configuring VMs on the host to maximize VM resource usage. (These counters are not automatically configured; you must configure them in the monitor if some advanced or optional configuration was performed in vCenter that you want to monitor.)

Monitor	Counter Name	Description
VMware Host CPU	usageToReservationRelation	Measures the relation between CPU usage and CPU reserved on the VM. If the counter value is $< 1$ over time, the VM is not using the reserved CPU and the vCenter administrator should consider reducing the reservation.
	usageToLimitRelation	Measures the relation between CPU usage and the CPU limit on the VM. If the counter value is $\geq 1$ (or close to 1) over time, the vCenter administrator should consider increasing the CPU limit for the VM.
VMware Host Memory	usageToReservationRelation	Measures the relation between memory usage and memory reserved on the VM.  If the counter value is $< 1$ over time, the VM is not using the reserved memory and the vCenter administrator should consider reducing the reservation.
	usageToLimitRelation	Measures the relation between memory usage and memory limit on the VM. If the counter value is $\geq 1$ (or close to 1) over time, the vCenter administrator should consider increasing the memory limit for the VM.
	usageOfESXMemory	Measures ESX host memory usage for every VM. This is useful for VMs that always run on the same ESX host (when there are no clusters or Distributed Resource Scheduler (DRS)).
	missingBalloonSizeTill Target	Measures the difference between the target balloon set for the VM (by the VMkernel) and the actual balloon size. If the counter value is $< 1$ over time, the VM uses more balloon size than was set as the target, and the vCenter administrator should consider increasing the target balloon size.

**Note:** If these smart counter values are unavailable, it means the values were not defined in vCenter (for example, a reservation or limit is not defined for the VM).

These counters provide the following information:

## 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 ["How to import the VMware Server Certificates" on page 741](#).

## Connection Pool Settings

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. The connection pool is a set of pools per key. A key is the combination of a vCenter or host

URL, and a user (the connection cannot be shared between different users due to different permissions).

If all VM monitors are configured with the same vCenter URL and user, one connection pool is created. For two vCenters and two different users for every vCenter, four connection pools are created.

The connection pool configures itself over time to ensure that only active connections stay in the pool. It does this by running an additional thread at the rate of the connection timeout multiplied by two; if the connection timeout is 30 minutes, it will run once every hour and evict idle connections from the pool. Connections that are idle for more than half a minute before the connection timeout are eligible for eviction.

For example, if the connection timeout is 30 minutes, the thread will evict connections that were idle for more than 29.5 minutes, but less than 30 minutes (to avoid a connection timeout). The connections that were idle more than 30 minutes are evicted by the timeout process. As a result, only active connections stay in the pool.

You can configure the following connection pool properties in **Preferences > Infrastructure Preferences > Custom Settings**:

- **VMware connection active connections in pool.** The maximum number of active connections in the pool. The default value is 60.
- **VMware connection initial timeout (seconds).** Connection initialization timeout in seconds. The default value is 30 seconds.
- **VMware connection minimum evictable idle time (minutes).** Minimum amount of time, in minutes, that VMware connection can be idle in the pool before it is eligible for eviction due to idle time. When a negative (-) number is set, no object will be dropped from the pool due to idle time. This setting has no effect unless VMware connection pool time between eviction runs (minutes) > 0. The default value is 30 minutes.
- **VMware connection pool time between eviction runs (minutes).** Interval, in minutes, between eviction thread runs for closing idle VMware connections. When a negative (-) number is set, no eviction thread is launched. The default value is 60 minutes.
- **VMware connection timeout (minutes).** Connection timeout in minutes. The default value is 30 minutes.
- **VMware connection total connections in pool.** The maximum number of connections (idle and active) in the pool.. The default value is 100.
- **VMware connection validate timeout (seconds).** Connection timeout, in seconds, for check connection operation. Validation is run, when VMware connection is pushed out from pool. The default value is 30 seconds.
- **VMware maximum idle connections in pool.** The maximum number of idle connections in the pool. The default value is 60.

**Tip:**

- We recommend setting the maximum size of total connections to the number of configured VM monitors in SiteScope, and let the internal connection pool mechanism optimize itself.
- If a SiteScope is registered to BSM, it uses more connections to retrieve properties relevant for topology reporting. Therefore, you should increase the maximum number of idle and active connection properties to enable SiteScope to perform well.

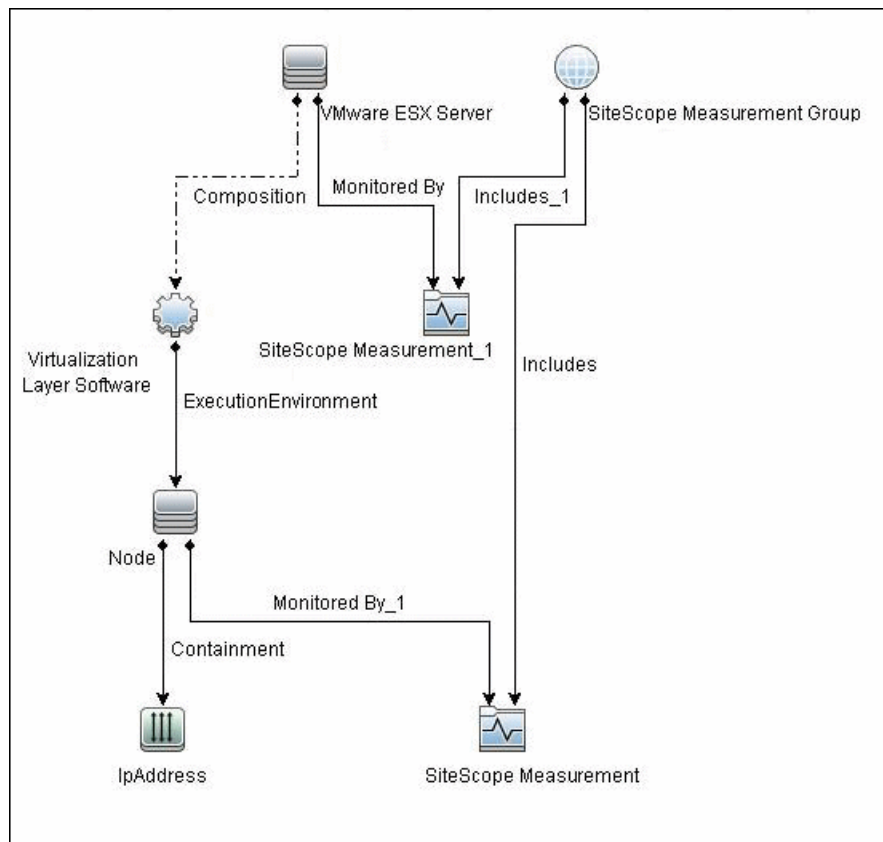
## VMotion Support

VMware's VMotion technology enables the 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.

## VMware Host Monitor Topology

The VMware Host monitors can identify the topology of the VMware servers being monitored. The monitor creates the following topology in BSM's RTSM.



For details on enabling topology reporting, see the task below.

The VMware Host monitor reports the Node CI for the virtual machine (VM) and the VMware ESX Server CI (ESX), and reports the connection between the VM and ESX. If there is counter defined on the VM, the related ESX is also reported.

### Note:

- When deleting a monitor or making configuration changes, links between previously reported VMs and ESXs are not deleted. This means that if a monitor was deleted and relevant VMs were subsequently migrated, the newly-created monitor contains the old link to the previous ESX Server and a link to the current ESX Server (reported on monitor creation).
- To enable the monitor to report the correct topology to BSM 9.0x, follow the ["VMware Host Monitors" on page 731](#) procedure in Troubleshooting and Limitations below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.



## System Tuning for Loaded Environments

SiteScope installed on a 64-bit environment supports configurations with up to 2150 VMware Host monitors running concurrently. This loaded system can be integrated with BSM and OM metrics.

To support loaded environments, the following system tuning is required:

- SiteScope sizing is required to increase JVM heap size, desktop heap size, and the number of file handles. You can use the SiteScope Configuration Tool to size SiteScope. For details, see [Using the SiteScope Configuration Tool in the SiteScope Deployment Guide](#) (<SiteScope root directory>\sisdocs\doc\_lib\Get\_Documentation.htm).
- It is recommended to connect directly using a host server rather than connecting to the VMware vCenter server.
- Add the **\_runGCPeriod=1200000** property to the <SiteScope root directory>\groups\master.config file. This means that SiteScope initiates running the garbage collector every 20 minutes (1200000 milliseconds) for better performance.
- Tune the vCenter/ESX connections parameters in **Preferences > Infrastructure Preferences > Custom Settings**, as required. For details, see ["Connection Pool Settings" on page 734](#).
- Increase the number of dynamic monitors handles in **Preferences > Infrastructure Preferences > Dynamic Monitoring Settings**:
  - **Dynamic monitoring core thread pool size**: 50
  - **Dynamic monitoring maximum thread pool size**: 70

## Metrics Integration Support

SiteScope uses the Operations Agent to make metrics data from VMware Host monitors available to Performance Manager in HPOM and to PMi in BSM.

The reported metrics are associated with the relevant ESX host or VM resource. The target is the counter target (not the monitor target).

Monitor Type	Reports Metrics For	Reports Metrics to the Following Tables
VMware Host	ESX	VMware Host CPU, Memory, Storage, State, Network, System tables
	VM	VMware VM CPU, Memory, Storage, State, Network, System tables

### Note:

- The first time you start monitoring a new VM or ESX host, it takes more time to get the data and to view it in the Operations Agent.
- To support motion and changes in the vCenter, such as change of IP or host name, you can change the interval for updating the data saved to the cache in the **Frequency of VM configuration retrieval from vCenter (hours)** field in **Preferences > Infrastructure Preferences > General Settings**. By default, data is updated every 4 hours. You can also configure this by modifying the **\_vmwareRetrieveConfFrequencyHours** property in the <SiteScope root directory>\groups\master.config file.

## License Consumption

Point-based Usage	Capacity-based Usage
<p>One point for each monitored VM or physical server.</p> <p>Note: While VMware Host monitors are supported by the OS Instance Advanced license, the license does not cover the ESX host and all VMs being monitored—it can be applied to one ESX host or VM (a separate OS license is required to cover each ESX host or VM). No points are consumed by each host or VM that is covered by the OS license.</p>	<p>One OS instance license per monitored host and one OS instance license for each monitored virtual machine. As a result, OSi capacity consumption for Dynamic VMware monitors can change during the monitor run according to the number of discovered VMs.</p> <p>VMware best practices recommend that you set the object name (in vSphere) of a VM guest to be the same as the server name (or machine name) of the guest itself. Where you set the names this way, SiteScope uses only one OSi for all monitors of the same server. Where the vSphere object name is different from the guest server name, SiteScope uses one OSi for all VMware monitors with the guest server name, and one OSi for all monitors with the vSphere object name.</p> <p>Note: Monitor is not available when using Community edition.</p>

## Tasks

This section includes:

- ["How to Configure the VMware Host Monitor" below](#)
- ["How to import the VMware Server Certificates" on page 741](#)


### How to Configure the VMware Host Monitor

#### 1. Prerequisites

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- The monitored vCenter or ESX server must be directly accessible by the SiteScope server (no proxy involved).
- The vCenter or ESX server provides a connection either by http or by https (depending on the vCenter or host server configuration). If https is used, server certificate must be imported to the SiteScope.

#### 2. 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. You can use one of the following methods for importing server certificates, or disable the requirement of having to import untrusted or invalid SSL certificates.


- Import the server certificates either:
  - Directly from the monitor using SiteScope's Certificate Management. In the monitor settings panel, click the **Import Certificates**  icon (next to the **vCenter URL/Host URL** box) to open the Import Certificates dialog box, and select the server certificates to import. For details, see step 2 of How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
  - Manually import the server certificates. For details, see ["How to import the VMware Server Certificates" on page 741](#).
- To use the monitor without having to import or check untrusted or invalid SSL certificates, select **VMware connection accept all untrusted certificates** in **Preferences > Infrastructure Preferences > Custom Settings**, and restart SiteScope. You must add the `_vmWareConnectionAcceptAllUntrustedCerts=true` property to the **master.config** file when upgrading from older versions of SiteScope.

### 3. Configure the monitor properties

For each VMware host, you can:

- Create the monitor by deploying the VMware Host solution template (recommended). The template contains a predefined monitor set with optimized settings that allow you to monitor only the relevant components. For solution template details, see VMware Host Solution Template in the Using SiteScope Guide.
- Create the monitor manually (as described in How to Deploy a Monitor in the Using SiteScope Guide), and then configure the settings as specified below.

#### To create the monitor manually:

- a. In the VMware Host Monitor Settings panel, enter the required vCenter or Host settings (for loaded environments, it is recommended to connect directly using a host server).  
For monitor user interface details, see ["VMware Host Monitor Settings" on page 742](#).
- b. Click the **Get Counter** button, and select the counters you want to monitor from the Select Counters Form. The counters are added to the Preview tree in the **Patterns & Counters** section.
- c. For dynamic monitoring, you can add patterns to counters to instruct the monitor which counters to use, either by:
  - Clicking the **Add New Counter**  button to add an empty line to the table, and creating a pattern format using a regular expression.

- The pattern should always start and end with the forward slash ("/") character.
- The "[" and "]" characters which appear as part of counter names should be escaped (preceded with the backslash ("\") character)
- Use ".\*" to describe any character any number of times.

For example, `./VirtualMachine/./cpu/usage.average\[ ]/` displays `usage.average[ ]` counter for all VMs.


- Selecting a static counter, and editing the counter to create a pattern format using a regular expression. For details on using regular expressions, see Regular Expressions Overview.

**Note:** For details on the maximum number of counters that can be selected from the browsable tree and the maximum number of counters that can match the selected counter

patterns when creating and updating dynamic monitors, see ["Troubleshooting and Limitations" on page 748](#). If the maximum number of counters that can be deployed is exceeded, an error is written to the **RunMonitor.log**.

**Example:**

If you enter the pattern `./VirtualMachine/./cpu/usage.average\[\]/`, the monitor retrieves the `usage.average[]` counter for all VMs.

- d. To view the counters that match a selected pattern, click the **View Matches for selected Pattern**  button. The matching counters are highlighted in the Counter Preview tree.
- e. Set the frequency for updating counters from the server in the **Frequency of updating counters from server** box. If you use only static counters, they are not affected by the frequency for updating counters, since the dynamic framework does not run.
- f. To display counters that no longer exist after the update mechanism runs, select **Continue displaying counters that no longer exist after update**. Any such counters are displayed as unavailable. This can be useful for keeping track of the counters that were previously being monitored.
- g. Click **Verify & Save** or **Save** to save your settings.
- h. In the **Threshold Settings** tab, you can manually set logic conditions for the dynamic counters that determine the reported status of each monitor instance. To view thresholds of all patterns translated to actual current counters, click the **Threshold Preview** button.

For threshold user interface details, see Threshold Settings in the Using SiteScope Guide.

**Note:** When configuring threshold settings for VMware Host monitors:

- The monitor **always(default)** counter configured in the **Good if** section of the monitor's properties means that the state of the monitor is good, unless one of the thresholds of any of the other counters is breached.
- The **countersinError** counter configured in the **Error if** section of the monitor's properties means that the state of the monitor is error if one of the other counters is unavailable.

#### 4. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["VMware Host Monitor Topology" on page 736](#).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

#### 5. Configure the connection pool mechanism - optional

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. We recommend setting the maximum size of total connections (in **Preferences > Infrastructure Preferences > Custom Settings > VMware connection active connections in pool**) to the number of configured VM monitors in SiteScope, and letting the internal connection pool mechanism optimize itself.

For details, see ["Connection Pool Settings" on page 734](#).

## 6. Results

If you are using the dynamic monitoring mechanism, during each update, the monitor connects to the vCenter/Host service and updates the status of each counter that matches the pattern defined by the regular expression. It also updates the thresholds for the selected counters.

You can check performance of the dynamic monitoring framework in:

- The **SiteScope Health** group, using the Dynamic Monitoring Statistics monitor. For details, see Dynamic Monitoring Statistics Page in the Using SiteScope Guide.
- In **Server Statistics** using the Dynamic Monitoring page. For details, see Dynamic Monitoring Page in the Using SiteScope Guide.


If counters are in error, try to isolate and troubleshoot the problem using the SiteScope VMware Host Best Practices document, which is available from `<SiteScope root directory>\sisdocs\pdfs\SiteScope_VMware_Host_Best_Practices.pdf`.

For additional troubleshooting suggestions, see ["Troubleshooting and Limitations" on page 748](#).

## How to 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 either:

- Manually using the keytool method (see procedure below for details).
- Directly from the monitor using SiteScope's Certificate Management. Click the **Import Certificates**  icon in the monitor settings panel to open the Import Certificates dialog box, and select the server certificates to import. For task details, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.

### 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.

# UI Descriptions

## VMware Host Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Connect by: vCenter</b>	<p>Select this option when connecting using a vCenter, and enter the following settings:</p> <ul style="list-style-type: none"><li>• <b>vCenter URL.</b> URL of the VMware vCenter infrastructure for the server you want to monitor. 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 vCenter server. You can import the server certificates directly from the monitor using SiteScope's Certificate Management (click the <b>Import Certificates</b> icon), instead of importing certificates manually.</li></ul> <p><b>Note:</b> If you get 'Error Code: 31008. Error getting counters' when SSL is used, navigate to <b>Preferences &gt; Infrastructure Preferences &gt; General Settings</b>, and select <b>Accept untrusted SSL certificates</b>.</p> <ul style="list-style-type: none"><li>• <b>ESX Host name.</b> Name of the ESX/ESXi host server you want to monitor.</li></ul> <p><b>Tip:</b> For loaded environments, it is recommended to connect directly using a host server rather than connecting to the VMware vCenter server.</p>
<b>Connect by: Host</b>	<p>Select this option when connecting directly using a host server, and enter the URL (host name, not IP address) of the VMware ESX host server you want to monitor in the <b>Host URL</b> box.</p> <p>You can import the server certificates directly from the monitor using SiteScope's Certificate Management (click the <b>Import Certificates</b> icon), instead of importing certificates manually.</p>
<b>Credentials</b>	<p>User name and password required to access the VMware Web service or host 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 How to Configure Credential Preferences in the Using SiteScope Guide.</li></ul>
<b>Host to take counters from</b>	<p>When working in template mode, enter the name of the VMware host server from which to take counters.</p> <p><b>Note:</b> This is available in Template mode only.</p>

UI Element	Description
<b>Patterns &amp; Counters</b>	<p>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p> <p>Click the <b>Add New Counter</b>  button to add an empty row at the bottom of the counters tree, enabling you to manually add a counter.</p> <p>Click the <b>Delete Counter</b>  button to remove the selected counters from the list. You can select multiple items using the CTRL or SHIFT keys.</p> <p>Click the <b>View Matches for Selected Pattern</b>  button to display counters that match the selected patterns.</p> <p><b>Note:</b> SiteScope uses Perl regular expressions for pattern matching. For example, if you enter <code>/cpu.*/</code> or <code>cpu</code>, any counters with <code>cpu</code> in their name match this pattern and are added to the counters list.</p>
<b>Get Counters</b>	<p>Opens a tree of all current counters, enabling you to select the counters you want to monitor. The tree is opened with no nodes selected. When you make a selection in the tree, the counters table is updated.</p> <p>For the list of counters that can be configured for the VMware Host monitors, see Monitor Counters.</p>
<b>Counter Preview</b>	<p>Displays all real counters in the monitor. This includes static counters and counter patterns that have been translated to real counters.</p>
<b>Frequency of updating counters from server</b>	<p>Time interval at which the counters that are requested by this monitor are retrieved from the server, and the monitor is updated with counter pattern matches. Use the drop-down list to specify increments of seconds, minutes, hours, or days.</p> <p><b>Default value:</b> 15 minutes</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The update frequency cannot be less than the monitor run frequency in Monitor Run Settings.</li> <li>• When configuring this setting in a template, the variable value can only be in time units of seconds.</li> <li>• Static counters are never deleted.</li> </ul>
<b>Continue displaying counters that no longer exist after update</b>	<p>Counters that no longer exist after running the update mechanism to retrieve counters from the VMware host server, are not deleted and are still displayed in the monitor (they are displayed as unavailable). This is useful if a server goes down or for keeping track of what counters were previously being monitored.</p> <p>When cleared, the counters that no longer exist are removed from the Counter Preview and Threshold Settings.</p> <p><b>Default value:</b> Selected</p>

## VMware Host to Take Counters From (Template mode only)

User interface elements are described below:

UI Element	Description
<b>Is vCenter</b>	Select when connecting using a vCenter.
<b>URL</b>	Enter the URL (host name, not IP address) of the VMware ESX host server you want to monitor.  You can import the server certificates directly from the monitor using SiteScope's Certificate Management (click the <b>Import Certificates</b> icon), instead of importing certificates manually.
<b>User name</b>	User name required to access the VMware host server.
<b>Password</b>	Password required to access the VMware host server.
<b>Host name</b>	Enter the name of the VMware host server from which to take counters. <b>Note:</b> This is available in Template mode only.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

### • VMware Host CPU

Below is the list of counters that can be configured for this monitor:

- ./.\*//HostSystem/cpu/idle.summation[]
- ./.\*//HostSystem/cpu/usage.average[]
- ./.\*//HostSystem/cpu/reservedCapacity.average[]
- ./.\*//HostSystem/cpu/wait.summation[]
- ./.\*//HostSystem/cpu/costop.summation[]
- ./.\*//HostSystem/cpu/swapwait.summation[]
- ./.\*//HostSystem/cpu/used.summation[]
- ./.\*//HostSystem/cpu/demand.average[]
- ./.\*//HostSystem/cpu/utilization.average[]
- ./.\*//HostSystem/cpu/totalCapacity.average[]
- ./.\*//HostSystem/cpu/ready.summation[]
- ./.\*//HostSystem/cpu/coreUtilization.average[]
- ./.\*//HostSystem/cpu/usagemhz.average[]
- ./.\*//HostSystem/cpu/latency.average[]
- ./.\*//VirtualMachine/.\*/usageToReservationRelation
- ./.\*//VirtualMachine/.\*/cpu/entitlement.latest\[ \]/
- ./.\*//VirtualMachine/.\*/cpu/usagemhz.average\[ \]/
- ./.\*//VirtualMachine/.\*/cpu/costop.summation\[ \]/
- ./.\*//VirtualMachine/.\*/cpu/latency.average\[ \]/
- ./.\*//VirtualMachine/.\*/cpu/maxlimited.summation\[ \]/



- `./VirtualMachine/.*/usageToLimitRelation`
- `./VirtualMachine/.*/cpu/overlap.summation\[\]/`
- `./VirtualMachine/.*/cpu/ready.summation\[\]/`
- `./VirtualMachine/.*/cpu/swapwait.summation\[\]/`
- `./VirtualMachine/.*/cpu/demand.average\[\]/`
- `./VirtualMachine/.*/cpu/run.summation\[\]/`
- `./VirtualMachine/.*/cpu/usage.average\[\]/`
- `./VirtualMachine/.*/cpu/used.summation\[\]/`
- `./VirtualMachine/.*/cpu/system.summation\[\]/`
- `./VirtualMachine/.*/cpu/idle.summation\[\]/`
- `./VirtualMachine/.*/cpu/wait.summation\[\]/`

## • VMware Host Memory

Below is the list of counters that can be configured for this monitor:

- `./HostSystem/mem/llSwapOutRate.average\[\]/`
- `./HostSystem/mem/llSwapIn.average\[\]/`
- `./HostSystem/mem/vmmemctl.average\[\]/`
- `./HostSystem/mem/granted.average\[\]/`
- `./HostSystem/mem/reservedCapacity.average\[\]/`
- `./HostSystem/mem/totalCapacity.average\[\]/`
- `./HostSystem/mem/heapfree.average\[\]/`
- `./HostSystem/mem/llSwapUsed.average\[\]/`
- `./HostSystem/mem/heap.average\[\]/`
- `./HostSystem/mem/llSwapInRate.average\[\]/`
- `./HostSystem/mem/latency.average\[\]/`
- `./HostSystem/mem/sysUsage.average\[\]/`
- `./HostSystem/mem/zero.average\[\]/`
- `./HostSystem/mem/active.average\[\]/`
- `./HostSystem/mem/swapoutRate.average\[\]/`
- `./HostSystem/mem/activewrite.average\[\]/`
- `./HostSystem/mem/shared.average\[\]/`
- `./HostSystem/mem/usage.average\[\]/`
- `./HostSystem/mem/unreserved.average\[\]/`
- `./HostSystem/mem/compressed.average\[\]/`
- `./HostSystem/mem/lowfreethreshold.average\[\]/`
- `./HostSystem/mem/consumed.average\[\]/`
- `./HostSystem/mem/state.latest\[\]/`
- `./HostSystem/mem/decompressionRate.average\[\]/`
- `./HostSystem/mem/compressionRate.average\[\]/`
- `./HostSystem/mem/swapinRate.average\[\]/`
- `./HostSystem/mem/overhead.average\[\]/`
- `./HostSystem/mem/swapused.average\[\]/`
- `./HostSystem/mem/swapout.average\[\]/`
- `./HostSystem/mem/swapin.average\[\]/`
- `./HostSystem/mem/sharedcommon.average\[\]/`
- `./HostSystem/mem/llSwapOut.average\[\]/`
- `./VirtualMachine/.*/usageToReservationRelation`
- `./VirtualMachine/.*/mem/llSwapInRate.average\[\]/`
- `./VirtualMachine/.*/mem/activewrite.average\[\]/`
- `./VirtualMachine/.*/mem/active.average\[\]/`

- `./VirtualMachine/.*/missingBalloonSizeTillTarget`
- `./VirtualMachine/.*/mem/llSwapOutRate.average\[/code>`
- `./VirtualMachine/.*/usageOfESXMemory`
- `./VirtualMachine/.*/mem/swapinRate.average\[/code>`
- `./VirtualMachine/.*/mem/usage.average\[/code>`
- `./VirtualMachine/.*/mem/swapin.average\[/code>`
- `./VirtualMachine/.*/mem/swapped.average\[/code>`
- `./VirtualMachine/.*/mem/shared.average\[/code>`
- `./VirtualMachine/.*/mem/zero.average\[/code>`
- `./VirtualMachine/.*/mem/swaptarget.average\[/code>`
- `./VirtualMachine/.*/usageToLimitRelation`
- `./VirtualMachine/.*/mem/vmmemctl.average\[/code>`
- `./VirtualMachine/.*/mem/entitlement.average\[/code>`
- `./VirtualMachine/.*/mem/zipSaved.latest\[/code>`
- `./VirtualMachine/.*/mem/granted.average\[/code>`
- `./VirtualMachine/.*/mem/zipped.latest\[/code>`
- `./VirtualMachine/.*/mem/swapoutRate.average\[/code>`
- `./VirtualMachine/.*/mem/overhead.average\[/code>`
- `./VirtualMachine/.*/mem/consumed.average\[/code>`
- `./VirtualMachine/.*/mem/overheadMax.average\[/code>`
- `./VirtualMachine/.*/mem/overheadTouched.average\[/code>`
- `./VirtualMachine/.*/mem/decompressionRate.average\[/code>`
- `./VirtualMachine/.*/mem/compressed.average\[/code>`
- `./VirtualMachine/.*/mem/compressionRate.average\[/code>`
- `./VirtualMachine/.*/mem/vmmemctltarget.average\[/code>`
- `./VirtualMachine/.*/mem/latency.average\[/code>`
- `./VirtualMachine/.*/mem/swapout.average\[/code>`
- `./VirtualMachine/.*/mem/llSwapUsed.average\[/code>`

## • VMware Host Network

Below is the list of counters that can be configured for this monitor:

- `./HostSystem/net/droppedRx.summation\[/code>`
- `./HostSystem/net/droppedTx.summation\[/code>`
- `./HostSystem/net/packetsRx.summation\[/code>`
- `./HostSystem/net/packetsTx.summation\[/code>`
- `./HostSystem/net/received.average\[/code>`
- `./HostSystem/net/transmitted.average\[/code>`
- `./HostSystem/net/usage.average\[/code>`
- `./VirtualMachine/.*/net/packetsRx.summation\[/code>`
- `./VirtualMachine/.*/net/packetsTx.summation\[/code>`
- `./VirtualMachine/.*/net/received.average\[/code>`
- `./VirtualMachine/.*/net/transmitted.average\[/code>`
- `./VirtualMachine/.*/net/usage.average\[/code>`

## • VMware Host State

Below is the list of counters that can be configured for this monitor:

- `./HostSystem/state/runtime.connectionState/`
- `./HostSystem/state/runtime.inMaintenanceMode/`
- `./HostSystem/state/hostSystem.fullName/`
- `./HostSystem/state/hardware.systemInfo.model/`

- ./HostSystem/state/hardware.memorySize/
- ./HostSystem/state/summary.hardware.numCpuCores/
- ./HostSystem/state/summary.hardware.cpuMhz/
- ./HostSystem/state/hardware.cpuPkg.description/
- ./HostSystem/state/config.network.pnic.linkSpeed.speedMb/
- ./HostSystem/state/systemResources.config.cpuAllocation.reservation/
- ./HostSystem/state/systemResources.config.cpuAllocation.limit/
- ./HostSystem/state/systemResources.config.cpuAllocation.shares.shares/
- ./HostSystem/state/systemResources.config.memoryAllocation.reservation/
- ./HostSystem/state/systemResources.config.memoryAllocation.limit/
- ./HostSystem/state/summary.hardware.uuid/
- ./HostSystem/state/summary.config.name/
- ./HostSystem/state/summary.hardware.numNics/
- ./HostSystem/sys/uptime.latest\[\]/
- ./VirtualMachine././state/ runtime.powerState/
- ./VirtualMachine././state/ guestinfo.guestFamily/
- ./VirtualMachine././state/ guestinfo.guestFullName/
- ./VirtualMachine././state/ guestinfo.guestId/
- ./VirtualMachine././state/ guestinfo.guestState/
- ./VirtualMachine././state/ guestinfo.ipAddress/
- ./VirtualMachine././state/ guestinfo.toolsVersion/
- ./VirtualMachine././state/ guest.hostName/
- ./VirtualMachine././state/config.hardware.memoryMB/
- ./VirtualMachine././state/ config.hardware.numCPU/
- ./VirtualMachine././state/config.cpuAllocation.reservation/
- ./VirtualMachine././state/ config.cpuAllocation.limit/
- ./VirtualMachine././state/config.cpuAllocation.shares.shares/
- ./VirtualMachine././state/config.memoryAllocation.reservation/
- ./VirtualMachine././state/config.memoryAllocation.limit/
- ./VirtualMachine././state/ config.uuid/
- ./VirtualMachine././state/ config.name/
- ./VirtualMachine././sys/ uptime.latest\[\]/

## • VMware Host Storage

Below is the list of counters that can be configured for this monitor:

- ./HostSystem/disk/numberWrite.summation\[\]/
- ./HostSystem/disk/totalLatency.average\[\]/
- ./HostSystem/disk/write.average\[\]/
- ./HostSystem/disk/queueReadLatency.average\[\]/
- ./HostSystem/disk/read.average\[\]/
- ./HostSystem/disk/deviceLatency.average\[\]/
- ./HostSystem/disk/totalReadLatency.average\[\]/
- ./HostSystem/disk/deviceWriteLatency.average\[\]/
- ./HostSystem/disk/queueLatency.average\[\]/
- ./HostSystem/disk/write.average\[\]/
- ./HostSystem/disk/busResets.summation\[\]/
- ./HostSystem/disk/queueWriteLatency.average\[\]/
- ./HostSystem/disk/kernelReadLatency.average\[\]/
- ./HostSystem/disk/commandsAveraged.average\[\]/
- ./HostSystem/disk/kernelWriteLatency.average\[\]/

- `./*/HostSystem/disk/read.average\[\]/`
- `./*/HostSystem/disk/numberReadAveraged.average\[\]/`
- `./*/HostSystem/disk/commands.summation\[\]/`
- `./*/HostSystem/disk/usage.average\[\]/`
- `./*/HostSystem/disk/numberRead.summation\[\]/`
- `./*/HostSystem/disk/kernelLatency.average\[\]/`
- `./*/HostSystem/disk/numberWriteAveraged.average\[\]/`
- `./*/HostSystem/disk/totalWriteLatency.average\[\]/`
- `./*/HostSystem/disk/commandsAborted.summation\[\]/`
- `./*/HostSystem/disk/deviceReadLatency.average\[\]/`
- `./*/HostSystem/disk/maxTotalLatency.latest\[\]/`
- `./*/VirtualMachine/./*/disk/numberWriteAveraged.average\[\]/`
- `./*/VirtualMachine/./*/disk/maxTotalLatency.latest\[\]/`
- `./*/VirtualMachine/./*/disk/usage.average\[\]/`
- `./*/VirtualMachine/./*/disk/busResets.summation\[\]/`
- `./*/VirtualMachine/./*/disk/commandsAborted.summation\[\]/`
- `./*/VirtualMachine/./*/disk/read.average\[\]/`
- `./*/VirtualMachine/./*/disk/numberRead.summation\[\]/`
- `./*/VirtualMachine/./*/disk/numberReadAveraged.average\[\]/`
- `./*/VirtualMachine/./*/disk/commands.summation\[\]/`
- `./*/VirtualMachine/./*/disk/commandsAveraged.average\[\]/`
- `./*/VirtualMachine/./*/disk/write.average\[\]/`
- `./*/VirtualMachine/./*/disk/numberWrite.summation\[\]/`
- `./*/VirtualMachine/./*/disk/read.average\[\]/`
- `./*/VirtualMachine/./*/disk/write.average\[\]/`

## Tips/Troubleshooting

### General Notes/Tips

- SiteScope supports configurations with up to 2150 VMware Host monitors.
- VMware Host Storage monitor does not support getting counter values from NFS-based storage.
- When deploying these monitors using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.
- When SiteScope is connected to BSM 9.00 or later, the **Indicator State and Severity** column is not displayed in Threshold Settings by default. This is because each counter pattern can affect more than one measurement, and only static counters and counter patterns are displayed by default. This column is displayed only when you click the **Threshold Preview** button (thresholds of all patterns are translated to actual current counters and are displayed).
- Baseline Settings are not available for dynamic monitors (these monitors configure their own thresholds).

### Troubleshooting and Limitations

This section describes troubleshooting and limitations for VMware Host monitors.

- ["Maximum Number of Counters That Can be Saved" on the next page](#)
- ["Incorrect ESX version displayed by the VMware Host State monitor" on the next page](#)
- ["Inaccurate Performance Analysis Using Perfmon to Monitor CPU on VMware " on the next page](#)

- ["Enable reporting Virtualization Layer Software CI when SiteScope is integrated with BSM 9.0x" on the next page](#)
- ["Wrong events are sent to OMi after a SiteScope restart" below](#)
- ["DNS Reconciliation Issues When Monitoring VMware-based Servers" on page 751](#)
- ["Troubleshooting Logs" on page 751](#)

## Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the **\_browsableContentMaxCounters** parameter in the **master.config** file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns is limited by the **\_maxCountersForRegexMatch** parameter in the **master.config** file. If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The **\_maxCountersForRegexMatch** parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both **\_browsableContentMaxCounters** and **\_maxCountersForRegexMatch** parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

## Incorrect ESX version displayed by the VMware Host State monitor

The incorrect ESX version is returned by the vCenter and displayed by the VMware Host State monitor. When the VMware Host State monitor monitors ESX directly (not via vCenter), the ESX version is correct.

## Inaccurate Performance Analysis Using Perfmon to Monitor CPU on VMware

**Problem:** SiteScope uses Perfmon to connect to the operating system of the VMware virtual machine and query it for CPU usage of the virtual host. When used over a period of time to monitor CPU on VMware, Perfmon provides inaccurate performance analysis.

**Solution:** VMware resolved this issue by integrating virtual machine performance counters such as CPU and memory into Perfmon for Microsoft Windows guest operating systems when VMware Tools is installed.

- For vSphere v4.0, install the latest version of VMware Tools from vSphere v4.0. When running the Windows perfmon utility, use the new counter groups, VM Processor and VM Memory, to see real CPU utilization.
- For VMs running on ESX/ESXi v3.5, contact VMware alliances for a standalone version of this Perfmon integration tool.

Use the VMware Host monitors to monitor the new counters groups to get accurate CPU utilization and memory data.

## Wrong events are sent to OMi after a SiteScope restart

**Problem:** VMware Host State monitor sends wrong events to OMi after a SiteScope restart.

The dynamic monitoring flow includes several separated steps (for example, step 1: counter changes, step 2: counter's topaz-ids change, step 3: topology change). When the first step ends, all other steps must be executed and must be completed properly. If only the first step is executed, the topology is not updated and the data in BSM will be incorrect.

**Solution:** Set the time to wait until all steps in the dynamic flow are completed (before SiteScope shutdown) in the `_timeToWaitToCompleteDynamicChangesOnSISShutdown` property in `<SiteScope root>\groups\master.config` file. By default, this key is hidden and the default value is 0 seconds. It is recommended to add a value of 120 (2 minutes). If the problem continues, increase the delay value.

## Enable reporting Virtualization Layer Software CI when SiteScope is integrated with BSM 9.0x

1. Update topology scripts.
  - a. In BSM 9.0x, select **Admin > RTSM Administration > Package Manager**, and export the **sitescope** package to a local directory. When the export process is complete, make a back up of the **sitescope.zip** file that is downloaded.
  - b. Extract the contents of **sitescope.zip** to a separate directory.
  - c. Extract the contents of `<SiteScope root directory>\conf\integration\bsm\BSM_90_VMwareHostMonitors.zip` to the `\discoveryScripts` folder of the directory used in the previous step (overwrite the existing script files).

**Note:** Make sure **sitescope.zip** consists only of the modified files under the `\discoveryScripts` folder.

- d. Archive the extracted structure. Make sure that the directory structure is the same as in the original file.
  - e. In BSM 9.0x, select **Admin > RTSM Administration > Package Manager**, and deploy the updated archive back to the server.
2. Update Indicator Assignments.

Perform the following steps for each of the 5 new monitors listed in the table below.

- a. In BSM, select **Admin > System Availability Management > Metrics and Indicators**, and click the **Select Monitor** button, and then click the **New Monitor** button.
- b. In the Add New Monitor dialog box, enter the display name, monitor class name, and category.

Monitor display name/Monitor topaz name	Monitor class name	Category
VMware Host CPU Monitor	VMwareHostCPUMonitor	Virtualization
VMware Host Memory Monitor	VMwareHostMemoryMonitor	Virtualization
VMware Host Network Monitor	VMwareHostNetworkMonitor	Virtualization
VMware Host State Monitor	VMwareHostStateMonitor	Virtualization
VMware Host Storage Monitor	VMwareHostStorageMonitor	Virtualization

- c. Import the **vmware host assignments.xml** file into the monitor indicator assignments.
  - d. Restart the SiteScope integrated with the BSM 9.0x server.

## DNS Reconciliation Issues When Monitoring VMware-based Servers

SiteScope performs DNS resolution to resolve new target hosts. When monitoring VMware-based servers, instead of using the DNS resolution mechanism, SiteScope resolves DNS using the VMware vCenter.

**Problem:** In some cases, there might be reconciliation issues. For example, when creating a new VM by cloning or deploying from a template, the new VM can be initialized with its parent VM\template DNS name.

However, for topology to be reported correctly, each VM name must represent its DNS name (the VM name must contain its short DNS name).

### Example:

```
VM1:
VM name: VMSiteScope1
DNS name: VMSiteScope1.hp.com

VM2:
VM name: VMSiteScope2
DNS name: VMSiteScope2Clone.hp.com
```

**Solution:** To enable correct topology reporting, you must set the `_shouldCheckIfVmDNSConfigured` property to `=true` in the `<SiteScope home>\groups\master.config` file.

## Troubleshooting Logs

1. Check for dynamic framework errors in:

- `<SiteScope root directory>\logs\dynamic_monitoring_changes.log`. This log describes monitor changes made by the dynamic framework (adding/removing counters), including the monitor name and counter name.
- `<SiteScope root directory>\logs\dynamic_monitoring.log`. This log describes all the tasks being run by the dynamic framework (counters extracted from the server, counters matched to patterns, and so on).

To check for dynamic monitoring errors, copy the following section from the `log4j.properties.debug` file in the `<SiteScope root directory>\conf\core\Tools\log4j\PlainJava` folder to the `log4j.properties` file, and change the log level to `DEBUG`.

```
#####
# Dynamic Monitoring
#####
log4j.category.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=
DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.DynamicBrowsableBase=false
log4j.category.com.mercury.sitescope.entities.monitors.dynamic=DEBUG, dynamic.monitoring.appender
log4j.additivity.com.mercury.sitescope.entities.monitors.dynamic=false
log4j.appender.dynamic.monitoring.appender=org.apache.log4j.RollingFileAppender
log4j.appender.dynamic.monitoring.appender.File=../${log.file.path}/dynamic_monitoring.log
log4j.appender.dynamic.monitoring.appender.MaxFileSize=1000KB
log4j.appender.dynamic.monitoring.appender.MaxBackupIndex=5
log4j.appender.dynamic.monitoring.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.dynamic.monitoring.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p - %m%n
```

2. Check for VMware monitor errors in:

- **<SiteScope root directory>\logs\RunMonitor.log**. Contains information about specific monitor runs and actions related to managing monitors.
- **<SiteScope root directory>\logs\vmware\_connections.log**. This log provides information about the connection pool against the ESX/vCenter (get/return connection).

To view VMware monitor errors, copy the following sections from the **log4j.properties.debug** file in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder to the **log4j.properties** file, and change the log level to DEBUG.

```
# VMware Connection Pool
#####
log4j.category.VMwareConnectionPool=${monitor.loglevel}, vmware.connection.pool.appender
log4j.additivity.VMwareConnectionPool=false
log4j.appender.vmware.connection.pool.appender=org.apache.log4j.RollingFileAppender
log4j.appender.vmware.connection.pool.appender.File=./${log.file.path}/vmware_connections.log
log4j.appender.vmware.connection.pool.appender.MaxFileSize=${def.file.max.size}
log4j.appender.vmware.connection.pool.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.vmware.connection.pool.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.vmware.connection.pool.appender.layout.ConversionPattern=%d [%t] (%F:%L) %-5p -
%m%n
```



# Chapter 109: VMware Performance Monitor

This monitor enables you to monitor performance statistics of the VMware infrastructure for various server applications.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the VMware Performance monitor.

## Learn About

This section includes:

- ["VMware Performance Monitor Overview" below](#)
- ["Supported Versions/Platforms" on the next page](#)
- ["VMware Performance Monitor or VMware Host Monitor?" on the next page](#)
- ["SSL Connectivity" on page 755](#)
- ["VMotion Support" on page 755](#)
- ["VMware Performance Topology" on page 755](#)
- ["System Tuning for Loaded Environments" on page 758](#)
- ["Metrics Integration Support" on page 760](#)
- ["License Consumption" on page 761](#)

## 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:

- ESX cluster, host, VM, and resource pool monitoring (it is not recommended to monitor more than one VM and ESX on a single monitor).
- 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>

**Tip:** To benefit from performance improvements made to this monitor, configure the filter options (**Get real-time data only**, **Get VMs and Hosts in powered on state only**, **Virtual machine**, and **Host**) according to the recommendations in ["How to Configure the VMware Performance Monitor" on page 763](#). For best practices details, see ["Best Practices for Configuring the VMware Performance Monitor" on page 761](#).

## Supported Versions/Platforms

This monitor supports monitoring remote servers running on:

- VMware VirtualCenter 2.x
- VMware ESX 3.x, 4.0, 4.1
- VMware ESXi 3.5, 4.0, 4.1, 5.0, 5.1, 5.5, 6.0
- VMware ESX 2.5 via VirtualCenter 2.x
- VMware ESX 3.x via VirtualCenter 3.x
- VMware vSphere 4.0, 4.1, 5.0, 5.1 (also supported with SSO login), 5.5, 6.0

**Note:** Monitoring VMware ESX(i) is not supported when Lockdown mode is enabled.

## VMware Performance Monitor or VMware Host Monitor?

	VMware Performance Monitor	VMware Host Monitors
<b>Type of user</b>	VM user/owner  <b>Note:</b> For vCenter Server 5.1 and 5.5, you can use a user with "Read-only" role.	Virtualization administrator  <b>Note:</b> For vCenter Server 5.1 and 5.5, you can use a user with "Read-only" role.
<b>Requirements</b>	<ul style="list-style-type: none"> <li>• Measure performance and availability of a particular VM or set of VMs.</li> <li>• Display SiteScope and BSM reports and BSM topology for this VM.</li> </ul> <p>Usually, VM users/owners are not interested on which host the VM runs or other issues.</p>	<ul style="list-style-type: none"> <li>• Manage a virtualization environment or vCenter and provide VM services to other users.</li> <li>• Measure the availability and performance of vCenter resources (physical host machines).</li> </ul> <p>Usually, virtualization administrators are not interested in specific VMs (only if this machine causes performance issues to the host).</p>
<b>Recommended Use</b>	Monitoring one or a set of VMs	Deploy using VM Host solution template
<b>Benefits</b>	Measures the data of every monitor run regardless of whether the VM has migrated.	<ul style="list-style-type: none"> <li>• Enables the administrator to make most efficient use of host resources (create maximum VMs and serve more users).</li> <li>• Provides notifications of availability and performance problems on the host (that might be caused by specific VM or VMs).</li> <li>• The monitor is dynamically updated (see <a href="#">"VMware Host Monitors" on page 731</a>).</li> <li>• Smart counters provide useful information for configuring the VM on the host to help maximize resource usage. For details, see <a href="#">"Smart Counters" on page 733</a>.</li> </ul>

	VMware Performance Monitor	VMware Host Monitors
<b>Data in SiteScope and BSM Reports</b>	Provides user with SiteScope and BSM reports with continuous data and topology that match the changes (the same VM connects to the relevant host).	<ul style="list-style-type: none"> <li>Enables the administrator to check host information only (the data is continuous). The topology matches VM migration for the monitored hosts.</li> <li>Does not provide continuous data on the VM (every time a VM migrates from host to host, its ID changes in SiteScope and BSM reports). However, VM data does not interest the administrator.</li> </ul>

## 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 ["How to import the VMware Server Certificates" on page 764](#).

## 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 browsable, 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.

**Tip:** When using the VM specific metrics, it is recommended to use the vCenter to support VMotion of the VM between ESX within the same vCenter.

You can set the interval for checking topology changes on the server in **HP Integration Settings > BSM Integration Data and Topology Settings**. Each time the monitor is run or updated, if the specified time since the last such server check has passed, the monitor checks the target server to see if migration of the monitored VMs has occurred.

## VMware Performance Topology

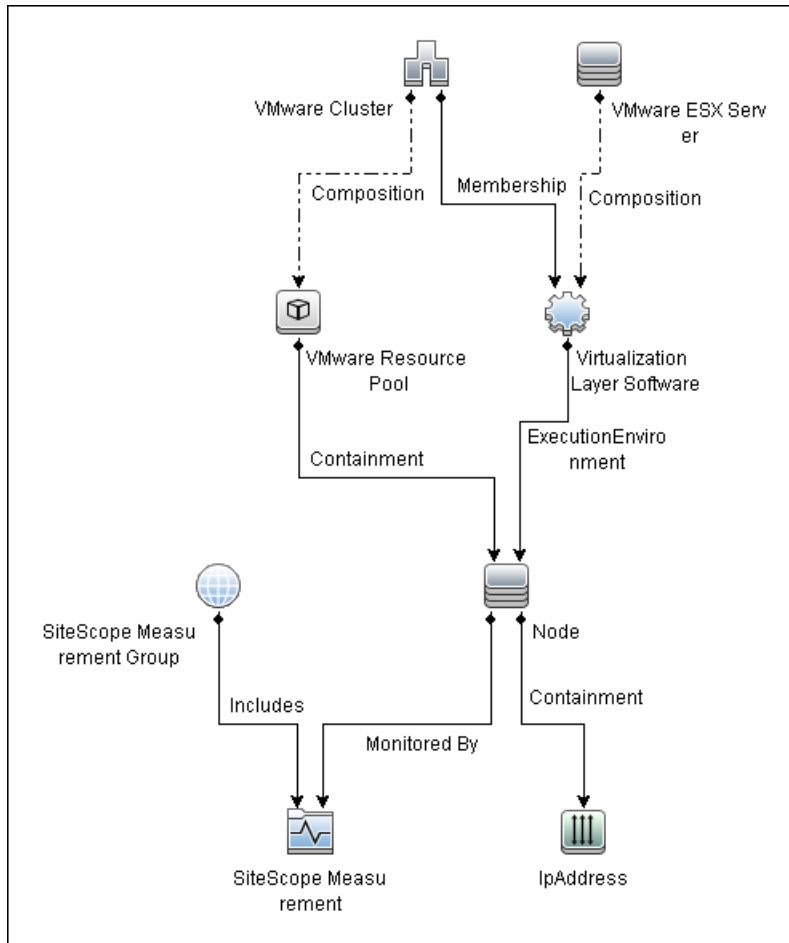
The VMware Performance monitor can identify the topology of the VMware servers being monitored. The monitor creates the following topology in BSM's RTSM.

The VMware Performance monitor reports the Node CI for the virtual machine (VM) and the VMware ESX Server CI (ESX), and reports the connection between the VM and ESX. If there is counter defined on the VM, the related ESX and resource pool are also reported.



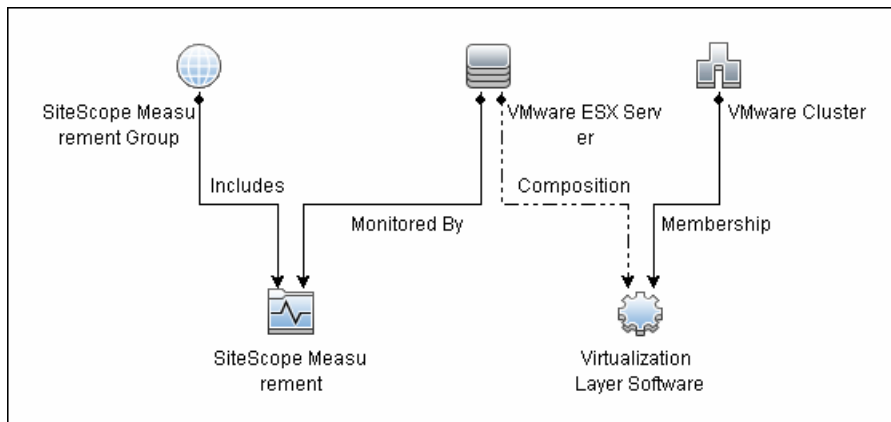
## Cluster to Virtual Machine

The VMware Performance monitor reports topology for the VMware Cluster to the VM.



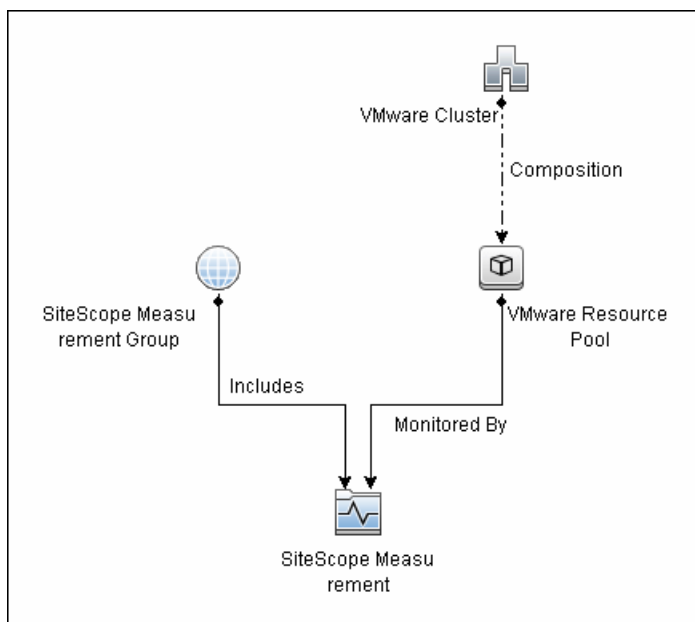
### Cluster to ESX Server

The VMware Performance monitor reports topology for the VMware Cluster to the ESX Server.



### Cluster to Resource Pool

The VMware Performance monitor reports topology for the VMware Cluster to the VMware Resource Pool.



For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

### System Tuning for Loaded Environments

SiteScope installed on a 64-bit environment supports configurations with up to 2150 VMware Performance monitors running concurrently. This loaded system can be integrated with BSM and OM metrics.

To support loaded environments, the following system tuning is required:

- SiteScope sizing is required to increase JVM heap size, desktop heap size, and the number of file handles. You can use the SiteScope Configuration Tool to size SiteScope. For details, see Using the

SiteScope Configuration Tool in the SiteScope Deployment Guide (<SiteScope root directory>\sisdocs\doc\_lib\Get\_Documentation.htm).

- Add the **\_runGCPeriod=1200000** property to the **<SiteScope root directory>\groups\master.config** file. This means that SiteScope initiates running the garbage collector every 20 minutes (1200000 milliseconds) for better performance.
- Tune the vCenter/ESX connections parameters in **Preferences > Infrastructure Preferences > Custom Settings**, as required. For details, see "[Connection Pool Settings](#)" on page 761.
- Increase the number of dynamic monitors handles in **Preferences > Infrastructure Preferences > Dynamic Monitoring Settings**:
  - **Dynamic monitoring core thread pool size**: 50
  - **Dynamic monitoring maximum thread pool size**: 70

## Metrics Integration Support

SiteScope uses the HP Operations agent to make metrics data from the VMware Performance monitor available to HP Performance Manager in HPOM and to Performance Graphing in BSM.

The reported metrics are associated with the relevant resource: ESX host, VM, or Resource Pool. The target is the counter target (not the monitor target).

Monitor Type	Reports Metrics For	Reports Metrics to the Following Tables
VMware Performance	ESX	VMware Host CPU, Memory, Storage, State, Network, System tables
	VM	VMware VM CPU, Memory, Storage, State, Network, System tables
	Resource Pool	VMware Resource Pool table

### Note:

- The first time you start monitoring a new VM or ESX host, it takes more time to get the data and to view it in the Operations Agent.
- The VMware Performance monitor supports the following metrics types only: CPU, disk, memory (mem), network (net), state and sys (system). All other metrics types are currently not supported, including general metrics such as `usageToPresevationRelation` and `usageToLimitRelation` metrics.
- By default, the VMware Performance monitor sends each metric to a specific table with its ESX host server, VM, or resource pool target, according to its data type. To revert back to the old behavior where the monitor sends all metrics to one table, clear the **Report VMware Performance monitor metrics to OA metrics classes** check box in **Preferences > Infrastructure Preferences > Monitor Settings**. You can also modify this setting in the `<SiteScope root directory>\groups\master.config` file by changing the `_omReportNewVmwareMetricClasses` property value to `=false`.
- To support motion and changes in the vCenter, such as change of IP or host name, you can change the interval for updating the data saved to the cache in the **Frequency of VM configuration retrieval from vCenter (hours)** field in **Preferences > Infrastructure Preferences > General Settings**. By default, data is updated every 4 hours. You can also configure this by modifying the `_vmwareRetrieveConfFrequencyHours` property in the `<SiteScope root directory>\groups\master.config` file.



## License Consumption

Points-based Usage	Capacity-based Usage
One point for each monitored VM or physical server. Note: No points are consumed by this monitor if it is running on a host covered by the OS Instance Advanced license.	One OSi license per monitored host

## Best Practices

### Best Practices for Configuring the VMware Performance Monitor

To benefit from performance improvements made to the VMware Performance monitor, you should configure the monitor filtering options and the connection pool settings according to the best practices below.

This section includes:

- ["Filtering Options" below](#)
- ["Connection Pool Settings" below](#)

### Filtering Options

To reduce monitor load on the VMware Performance monitor, it is important to use the appropriate filtering settings when configuring the monitor settings. If filtering options are not used, the monitor is placed under enormous load as it creates an XML file with all the counters retrieved. This causes performance problems each time monitor properties are opened, since the monitor attempts to display a large number of counters and create a heavy cache file.

When configuring the monitor, you should:

- Enter a virtual machine and host name in the **Virtual machine** and **Host** fields. If these fields are not filled, the monitor attempts to retrieve counters for all VMs, hosts, and resource pools defined in the vCenter. For example, if a vCenter has 800 VMs and 100 hosts, the monitor will try to get 80 counters per VM and 90 counters per host (this is the average number - the actual number depends on the configuration of the VM or host and may be even higher). In total: (800 VMs x 80 counters) + (100 Hosts x 90 counters) = 73,000 counters.
- Make sure that the **Get real-time data only** option is selected (it is selected by default) so that historical data is not included. The number of counters above represents real-time data only. This number could be much higher, depending on your configuration, if historical data is not excluded.
- To avoid retrieving historical data from powered off VMs and hosts, make sure that the **Get VMs and Hosts in powered on state only** option is selected (it is selected by default).

For details on configuring filtering options, see ["How to Configure the VMware Performance Monitor" on page 763](#).

### Connection Pool Settings

The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. The connection pool is a set of pools per key. A key is the combination of a vCenter or host URL, and a user (the connection cannot be shared between different users due to different permissions).

If all VMware Performance monitors are configured with the same vCenter URL and user, one connection pool is created. For two vCenters and two different users for every vCenter, four connection pools are created.

The connection pool configures itself over time to ensure that only active connections stay in the pool. It does this by running an additional thread at the rate of the connection timeout multiplied by two; if the connection timeout is 30 minutes, it will run once every hour and evict idle connections from the pool. Connections that are idle for more than half a minute before the connection timeout are eligible for eviction.

For example, if the connection timeout is 30 minutes, the thread will evict connections that were idle for more than 29.5 minutes, but less than 30 minutes (to avoid a connection timeout). As a result, only active connections stay in the pool.

You can configure the following connection pool settings in **Preferences > Infrastructure Preferences > Custom Settings**:

- **VMware connection active connections in pool.** The maximum number of active connections in the pool. The default value is 60.
- **VMware connection initial timeout (seconds).** Connection initialization timeout in seconds. The default value is 30 seconds.
- **VMware connection minimum evictable idle time (minutes).** Minimum amount of time, in minutes, that VMware connection can be idle in the pool before it is eligible for eviction due to idle time. When a negative (-) number is set, no object will be dropped from the pool due to idle time. This setting has no effect unless VMware connection pool time between eviction runs (minutes) > 0. The default value is 30 minutes.
- **VMware connection pool time between eviction runs (minutes).** Interval, in minutes, between eviction thread runs for closing idle VMware connections. When a negative (-) number is set, no eviction thread is launched. The default value is 60 minutes.
- **VMware connection timeout (minutes).** Connection timeout in minutes. The default value is 30 minutes.
- **VMware connection total connections in pool.** The maximum number of connections (idle and active) in the pool.. The default value is 100.
- **VMware connection validate timeout (seconds).** Connection timeout, in seconds, for check connection operation. Validation is run, when VMware connection is pushed out from pool. The default value is 30 seconds.
- **VMware maximum idle connections in pool.** The maximum number of idle connections in the pool. The default value is 60.

**Tip:**

- We recommend setting the maximum size of total connections to the number of configured VM monitors in SiteScope, and let the internal connection pool mechanism optimize itself.
- If a SiteScope is registered to BSM, it uses more connections to retrieve properties relevant for topology reporting. Therefore, you should increase the maximum number of idle and active connection properties to enable SiteScope to perform well.

## Tasks

This section includes:

- ["How to Configure the VMware Performance Monitor" on the next page](#)
- ["How to import the VMware Server Certificates" on page 764](#)

## How to Configure the VMware Performance Monitor

### 1. Prerequisites

The following are the requirements for monitoring VMware-based servers:

- The monitored vCenter or ESX server must be directly accessible by the SiteScope server (no proxy involved).
- The vCenter server or ESX server provides connection either by http or by https (depending on the vCenter/host server configuration). If https is used, server certificate must be imported to the SiteScope.

### 2. 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. You can use one of the following methods for importing server certificates, or disable the requirement of having to import untrusted or invalid SSL certificates.

- Import the server certificates either:
  - Using Certificate Management in SiteScope (avoids having to restart SiteScope). For details, see step 2 of How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
  - Manually import the server certificates. For details, see ["How to import the VMware Server Certificates" on the next page](#).
- To use the monitor without having to import or check untrusted or invalid SSL certificates, select **VMware connection accept all untrusted certificates** in **Preferences > Infrastructure Preferences > Custom Settings**, and restart SiteScope. You must add the `_vmWareConnectionAcceptAllUntrustedCerts=true` property to the `master.config` file when upgrading from older versions of SiteScope.

### 3. Configure the monitor properties

To benefit from performance improvements made to this monitor, configure the monitor according to the recommendations below. For best practices details, see ["Best Practices for Configuring the VMware Performance Monitor" on page 761](#).

- a. Create a separate monitor for each VM or host. (This is because the monitor is limited to monitoring 100 counters, and every VM or host has an average of 80-90 counters.)

For task details on adding a monitor, see How to Deploy a Monitor in the Using SiteScope Guide.

- b. Configure the following filter options to avoid overloading the monitor:

For Virtual machine:

- **Get real-time data only:** Selected
- **Get VMs and Hosts in powered on state only:** Selected
- **Host:** /--/
- **Virtual machine:** < Enter VM name >

For Host:

- **Get real-time data only:** Selected
- **Get VMs and Hosts in powered on state only:** Selected

- **Host:** <Enter host name>
  - **Virtual machine:** /--/
- c. Configure the other monitor properties as required.  
For user interface details, see the UI Descriptions section below.

#### 4. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["VMware Performance Topology" on page 755](#).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

#### 5. Configure the connection pool mechanism - optional


The connection pool mechanism reduces the load on VMware infrastructure and SiteScope by optimizing connections. We recommend setting the maximum size of total connections (in **Preferences > Infrastructure Preferences > Custom Settings > VMware connection active connections in pool**) to the number of configured VM monitors in SiteScope, and letting the internal connection pool mechanism optimize itself.

For details, see ["Connection Pool Settings" on page 761](#).

### How to 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 either:

- Manually using the keytool method (see procedure below for details).
- Directly from the monitor using SiteScope's Certificate Management. Click the **Import Certificates**  icon in the monitor settings panel to open the Import Certificates dialog box, and select the server certificates to import. For task details, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.

#### To manually import server certificates:

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.

## UI Descriptions

### VMware Performance Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>URL</b>	<p>URL of 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</p> <p>where &lt;protocol&gt; is either http or https, and &lt;server_name&gt; is the name of the vCenter or ESX server. You can import the server certificates directly from the monitor using SiteScope's Certificate Management (click the <b>Import Certificates</b> icon), instead of importing certificates manually.</p> <p><b>Note:</b> If you get 'Error Code: 31008. Error getting counters' when SSL is used, navigate to <b>Preferences &gt; Infrastructure Preferences &gt; General Settings</b>, and select <b>Accept untrusted SSL certificates</b>.</p>
<b>Credentials</b>	<p>User name and password required to access the VMware Web service. 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 How to Configure Credential Preferences in the Using SiteScope Guide.</li> </ul>
<b>Get real-time data only</b>	<p>Select to retrieve real-time metrics data only and exclude historical metrics data.</p> <p><b>Default value:</b> Selected</p>
<b>Get VMs and Hosts in powered on state only</b>	<p>Select to retrieve metrics data from powered on VMs and hosts only (data from powered off VMs/hosts is excluded).</p> <p><b>Default value:</b> Selected.</p>
<b>Host</b>	<p>Enter a regular expression to match the name of one or more hosts. Only hosts that match this expression are displayed in the Counters list. Click the <b>Open Tool</b> button to use the Regular Expression tool to check the correctness of your regular expression.</p>

UI Element	Description
<b>Virtual machine</b>	Enter a regular expression to match the name of one or more virtual machines. When you apply this filter, only the virtual machines that match this string are displayed in the Get Counters list. Click the <b>Open Tool</b> button to use the Regular Expression tool to check the correctness of a regular expression.
<b>Counter Settings</b>	
<b>Counters</b>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.  <b>Tip:</b> When using the VM specific metrics, it is recommended to use the vCenter to support VMotion of the VM between ESX within the same vCenter.
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a> .  <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.

## HP Integration Settings (for VMware Performance Monitor)

The setting below is specific to the VMware Performance monitor. For HP Integration Settings common to all monitors, see HP Integration Settings in the Using SiteScope Guide.

UI Element	Description
<b>BSM Integration Data and Topology Settings</b>	
<b>Interval to check server for topology changes (minutes)</b>	Each time the monitor is run or updated, if the specified time since the last such server check has passed, the monitor checks the target server to see if migration of the monitored VMs has occurred. If it has, it updates the relationship of monitored VMs to the ESX servers on which they are running.  <b>Default value:</b> 60 minutes

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

<p><b>CPU Usage (Group: cpu)</b></p> <ul style="list-style-type: none"> <li>• usage</li> <li>• usagemhz</li> <li>• system</li> <li>• wait</li> <li>• ready</li> <li>• extra</li> <li>• used</li> <li>• guaranteed</li> <li>• reservedCapacity</li> </ul> <p><b>CPU Utilization for Resources (Group: rescpu)</b></p> <ul style="list-style-type: none"> <li>• actav1</li> <li>• actav5</li> <li>• actav15</li> <li>• actpk1</li> <li>• actpk5</li> <li>• actpk15</li> <li>• runav1</li> <li>• runav5</li> <li>• runav15</li> <li>• runpk1</li> <li>• runpk5</li> <li>• runpk15</li> <li>• maxLimited1</li> <li>• maxLimited5</li> <li>• maxLimited15</li> <li>• sampleCount</li> <li>• samplePeriod</li> </ul> <p><b>Memory Performance (Group: mem)</b></p> <ul style="list-style-type: none"> <li>• usage</li> <li>• vmmemctl</li> <li>• active</li> <li>• granted</li> <li>• shared</li> <li>• zero</li> <li>• unreserved</li> <li>• swapunreserved</li> <li>• swapused</li> <li>• sharedcommon</li> <li>• heap</li> <li>• heapfree</li> </ul>	<ul style="list-style-type: none"> <li>• state</li> <li>• swapped</li> <li>• swaptarget</li> <li>• swapin</li> <li>• swapout</li> <li>• vmmemctltarget</li> <li>• consumed</li> <li>• overhead</li> <li>• reservedCapacity</li> </ul> <p><b>Network Performance (Group: net)</b></p> <ul style="list-style-type: none"> <li>• usage</li> <li>• transmitted</li> <li>• received</li> <li>• packetRx</li> <li>• packetTx</li> </ul> <p><b>Disk Performance (Group: disk)</b></p> <ul style="list-style-type: none"> <li>• usage</li> <li>• read</li> <li>• write</li> <li>• numberRead</li> <li>• numberWrite</li> </ul> <p><b>System Performance (Group: sys)</b></p> <ul style="list-style-type: none"> <li>• uptime</li> <li>• resourceCpuUsage</li> <li>• heartbeat</li> </ul> <p><b>Cluster Services Metrics (Group: clusterServices)</b></p> <ul style="list-style-type: none"> <li>• cpufairness</li> <li>• memfairness</li> </ul> <p><b>Cluster State Metrics (Group: ClusterComputeResource/state)</b></p> <ul style="list-style-type: none"> <li>• summary.effectiveCpu</li> <li>• summary.effectiveMemory</li> <li>• summary.numCpuCores</li> <li>• summary.numCpuThreads</li> <li>• summary.numEffectiveHosts</li> <li>• summary.overallStatus</li> <li>• summary.totalCpu</li> <li>• summary.totalMemory</li> <li>• summary.numHosts</li> </ul>
---	--

<p><b>Resource Pools State Metrics (Group: Resource Pools /state)</b></p> <ul style="list-style-type: none"> <li>• name</li> <li>• config.memoryAllocation.reservation</li> <li>• config.memoryAllocation.limit</li> <li>• config.cpuAllocation.reservation</li> <li>• config.cpuAllocation.limit</li> <li>• config.cpuAllocation.shares.shares</li> </ul> <p><b>Host State Metrics (Group: Host System/state)</b></p> <ul style="list-style-type: none"> <li>• runtime.connectionState</li> <li>• runtime.in runtime.inMaintenanceMode</li> <li>• summary.config.product.fullName</li> <li>• hardware.systemInfo.model</li> <li>• hardware.memorySize</li> <li>• summary.hardware.numCpuCores</li> <li>• summary.hardware.cpuMhz</li> <li>• hardware.cpuPkg.description</li> <li>• config.network.pnic.linkSpeed.speedMb</li> <li>• systemResources.config.cpuAllocation.reservation</li> <li>• systemResources.config.cpuAllocation.limit</li> <li>• systemResources.config.cpuAllocation.shares.shares</li> <li>• systemResources.config.memoryAllocation.reservation</li> <li>• systemResources.config.memoryAllocation.limit</li> <li>• summary.hardware.uuid</li> <li>• summary.config.name</li> <li>• summary.hardware.numNics</li> </ul>	<p><b>Virtual Machine State Metrics (Group: VirtualMachine/state)</b></p> <ul style="list-style-type: none"> <li>• runtime.powerState</li> <li>• guest.guestFamily</li> <li>• guest.guestFullName</li> <li>• guest.guestId</li> <li>• guest.guestState</li> <li>• guest.ipAddress</li> <li>• guest.hostName</li> <li>• guest.toolsVersion</li> <li>• config.hardware.memoryMB</li> <li>• config.hardware.numCPU</li> <li>• config.cpuAllocation.reservation</li> <li>• config.cpuAllocation.limit</li> <li>• config.cpuAllocation.shares.shares</li> <li>• config.memoryAllocation.reservation</li> <li>• config.memoryAllocation.limit</li> <li>• config.uuid</li> <li>• config.name</li> </ul>
--	--

## Tips/Troubleshooting

### General Notes/Tips

- For VMware Performance monitors that were configured in earlier versions of SiteScope, the **Get real-time data only** and **Get VMs and Hosts in powered on state only** options are not selected by default.
- When deploying this monitor using a template, clearing the **Verify monitor properties with remote server** option deploys the monitor without connecting to the server, thereby enabling template deployment on powered on and powered off VMs. When this option is selected (the default setting), deployment fails for VMs that are not powered on.
- The CPU shares counter in the resource pool (**Resource Pool > summary > config > cpuAllocation > shares > shares**) displays a value of 0 instead of the actual number of shares allocated if level is not set to custom on the VMware server. For more details, see the VMware support site (<http://www.vmware.com/support/developer/vc-sdk/visdk41pubs/ApiReference/vim.SharesInfo.html>).

### Troubleshooting and Limitations

This section contains the following troubleshooting issues:

- ["Counter Errors After SiteScope Upgrade" on the next page](#)
- ["Inaccurate Performance Analysis Using Perfmon to Monitor CPU on VMware " on the next page](#)
- ["DNS Reconciliation Issues When Monitoring VMware-based Servers" on the next page](#)



## Counter Errors After SiteScope Upgrade

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.

## Inaccurate Performance Analysis Using Perfmon to Monitor CPU on VMware

**Problem:** SiteScope uses Perfmon to connect to the operating system of the VMware virtual machine and query it for CPU usage of the virtual host. When used over a period of time to monitor CPU on VMware, Perfmon provides inaccurate performance analysis.

**Solution:** VMware resolved this issue by integrating virtual machine performance counters such as CPU and memory into Perfmon for Microsoft Windows guest operating systems when VMware Tools is installed.

- For vSphere v4.0, install the latest version of VMware Tools from vSphere v4.0. When running the Windows perfmon utility, use the new counter groups, VM Processor and VM Memory, to see real CPU utilization.
- For VMs running on ESX/ESXi v3.5, contact VMware alliances for a standalone version of this Perfmon integration tool.

Use the VMware Performance monitor to monitor the new counters groups to get accurate CPU utilization and memory data.

## DNS Reconciliation Issues When Monitoring VMware-based Servers

SiteScope performs DNS resolution to resolve new target hosts. When monitoring VMware-based servers, instead of using the DNS resolution mechanism, SiteScope resolves DNS using the VMware vCenter.

**Problem:** In some cases, there might be reconciliation issues. For example, when creating a new VM by cloning or deploying from a template, the new VM can be initialized with its parent VM\template DNS name.

However, for topology to be reported correctly, each VM name must represent its DNS name (the VM name must contain its short DNS name).

### Example:

```
VM1:
VM name: VMSiteScope1
DNS name: VMSiteScope1.hp.com

VM2:
VM name: VMSiteScope2
DNS name: VMSiteScope2Clone.hp.com
```

**Solution:** To enable correct topology reporting, you must set the **\_shouldCheckIfVmDNSConfigured** property to **=true** in the **<SiteScope home>\groups\master.config** file.

# Chapter 110: Web Script Monitor

The Web Script monitor provides 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Web Script monitor.

## Learn About

This section includes:

- ["Web Script Monitor Overview" below](#)
- ["Supported Platforms/Versions" on the next page](#)
- ["Counter Measurements and Transaction Breakdown Data" on the next page](#)
- ["Working with VuGen" on the next page](#)
- ["Advanced Information" on page 774](#)
- ["Web Script Performance Counters" on page 774](#)
- ["License Consumption" on page 776](#)

## 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.

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 use a back-end database).

The Web Script monitor runs the scripts created in the 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 the next page](#).

To run the script, the Load Generator must be installed on the SiteScope server. To use this monitor with SiteScope Failover, you must install the same version of the Load Generator on the Failover server and specify the path in **Preferences > Infrastructure Preferences > Custom Settings** or in `_loadGeneratorPath=` in the `<SiteScope root>\groups\master.config` file.

**Note:** The Web Script monitor's data cannot be reported to BSM.

## Supported Platforms/Versions

- This monitor is supported in SiteScopes running on Windows and Linux 64-bit environments (SiteScope is no longer supported on 32-bit operating systems).
- This monitor supports scripts created in VuGen version 12.02 (scripts created in VuGen versions 9.51 and earlier are retained for backward compatibility).
- From SiteScope 11.30 onwards: To use the Web Script monitor, you must install HP Load Generator 12.02 on the SiteScope server to run web scripts.

For details on downloading VuGen 12.02 and HP Load Generator 12.02, see ["How to Configure the Web Script Monitor" on page 776](#).

## 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.

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 the counter metrics available for the monitor, see ["Web Script Performance Counters" on page 774](#).

## 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.

This section also includes:

- ["Getting Started" below](#)
- ["Supported VuGen Protocols" below](#)
- ["Inserting Transactions and Creating Checkpoints" on the next page](#)
- ["Saving and Storing the Script" on the next page](#)

## 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 Virtual User Generator guide.

For more detailed information on creating scripts, refer to "Working with VuGen" > "Recording with VuGen" > "Creating New Virtual User Scripts" in the Virtual User Generator guide.

## Supported VuGen Protocols

The following are the protocols supported for the Web Script monitor when VuGen scripts are invoked by SiteScope:

- ["Ajax \(Click and Script\) Protocol" below](#)
- ["Web \(HTTP/HTML\) Protocol" on the next page](#)

### Ajax (Click and Script) Protocol

This is the recommended protocol to use to record scripts to be run by the Web Script monitor.

Ajax (Click and Script) is a new approach to Web scripting. It introduces a user interface-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 Ajax (Click and Script) Vuser Scripts" sections under "E-Business Protocols" in the Virtual User Generator guide.

For the browsers supported for recording and emulating web scripts, refer to the relevant version of the Virtual User Generator guide or the HP Load Generator guide (available from the [HPE Software Support site](#)).

### Limitations:

- 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.

- Recording of an application in a specific language (for example, French, Japanese) must be performed on a machine whose default locale (in **Control Panel >Regional Options**) is the same language.
- Due to a lack of AJAX/other frameworks in VuGen 9.51 Web (Click and Script) protocols, you might encounter a memory violation error. Therefore, you should upgrade to VuGen 12.02.

**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 Virtual User Generator 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 Virtual User Generator 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 Virtual User Generator 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 Virtual User Generator 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 Virtual User Generator 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 > General Settings**). 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.

## Advanced Information

The Web Script monitor uses the Load Generator 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 **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.

## 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>	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.  Retry time only relates to HTTP or TCP errors that execute a retry after the error.
<b>Retry Count</b>	Displays the number of times an HTTP request is returned.
<b>DNS Time</b>	Displays the average amount of time needed to resolve the DNS name to an IP address, using the closest DNS server.  The DNS Lookup measurement is a good indicator of slow DNS resolution or other problems with the DNS server.

Name	Description
<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>
<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>Total/Status</b>	Displays whether the script passed or failed. A value of 0 is passed, a value of 1 is failed. A failed script 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.

Name	Description
<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.
<b>Transaction think time</b>	The time taken for each transaction (that is, the time between action requests, which is calculated as the total think time duration produced by all <code>lr_think_time()</code> function entries in some specific transaction). Think time varies depending on the application context. It is not advisable to have the default think time for all applications under testing.
<b>Transaction wasted time</b>	The difference between actual time spent on processing and displaying information and idle or waiting time.
<b>Transaction start time</b>	Time when the transaction started.
<b>Transaction end time</b>	Time when the transaction ended.

## License Consumption

Points-based Usage	Capacity-based Usage
<p>Four points per transaction run by the monitor.</p> <p>A transaction can include as many URLs as needed. The monitor can include up to 12 measurements per transaction.</p> <p>Note: A Web Script monitor can consume more than 4 points if a script run by the monitor has more than 1 transaction.</p>	<p>One transaction license per monitored host.</p> <p>Note: Monitor is not available when using Community or Load Testing edition.</p>

# Tasks

## How to Configure the Web Script Monitor

1. Prerequisites
  - a. Install Load Generator 12.02 on the SiteScope server to run web scripts.
    - i. Go to the My Software Updates portal (<https://h20575.www2.hp.com/usbportal/softwareupdate.do>), select **SiteScope** in the SAID Products list, and click **View available products**.
    - ii. Expand **Application Performance Management**, select the SiteScope version you require, and click **Get software updates**.
    - iii. In the **Selected Products** tab, click **Get Software** for the product you want.
    - iv. In the **Downloads** section, select **HP Load Generator 12.02 for Windows/Linux**, and follow the instructions on the site to download the software.
  - b. After Load Generator is installed, specify the path to the mdrv executable file in **Preferences >**



**Infrastructure Preferences > Custom Settings > loadGeneratorPath** (or add the path to `_loadGeneratorPath=` in the `<SiteScope root>\groups\master.config` file).

Path example:

On Windows: `C:\temp\HPLoadGenerator12.02\HP\Load Generator\bin\mdrv.exe`

On Linux: `/opt/HP/HP_LoadGenerator/bin/mdrv`

- c. Restart SiteScope.

**Note:**

- If import Web Script monitors from an earlier version of SiteScope and you have not performed the above steps, an error message is displayed in the monitor status. To remedy the issue, install the Load Generator and specify the path to the Load Generator executable file (mdrv).
- To use this monitor with SiteScope Failover, you must install the same version of the Load Generator on the Failover server, and specify the path in **Preferences > Infrastructure Preferences > Custom Settings > loadGeneratorPath** or add the path to `_loadGeneratorPath=` in the `<SiteScope root>\groups\master.config` file.

2. Create a script using Virtual User Generator (VuGen)

Prior to configuring the Web Script monitor in SiteScope, you must create the script in VuGen (only scripts created using VuGen 12.02 are supported).

- a. Download VuGen 12.02.

Follow the instructions in Prerequisites above, and in the **Downloads** section, select **HP VuGen 12.02 for Windows**.

- 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" in ["Working with VuGen" on page 771](#).

- 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" in ["Working with VuGen" on page 771](#).

- 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 Virtual User Generator 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 Virtual User Generator 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" in ["Working with VuGen" on page 771](#).

- 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 Virtual User Generator guide.

3. Create the monitor and configure the monitor properties.

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** When configuring the monitor, make sure you set a monitor frequency that provides sufficient time for the Load Generator to completely run the web script and generate output. For large web scripts, we recommend using the default monitor frequency (15 minutes).

## UI Descriptions

### Web Script Monitor Settings

User interface elements are described below:

UI 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 <b>&lt;SiteScope root directory&gt;\templates.webscripts</b> or a directory you name in <b>VuGen scripts path root</b> in General Preferences. For details, see General Preferences in the Using SiteScope Guide.</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>Amount of 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>
<b>Counters</b>	<p>Displays the server performance counters you want to check with this monitor. Use the <b>Get Counters</b> button to select counters.</p>

UI Element	Description
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters available for the monitor, see <a href="#">"Web Script Performance Counters" on page 774</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### Troubleshooting and Limitations

This section describes troubleshooting and limitations for the Web Script monitor.

- Web Script monitors running on a Linux-based SiteScope do not support old scripts (from VuGen 9.5 or earlier); they only support scripts generated using VuGen 12.02.
- 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\persistent\WebScript\<name of script>\<unique ID>\res**. 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.  
By default, historical logging is disabled (only the last run is saved). To enable historical logging, add the **\_mdrvLogHistoryAppend** property to the **<SiteScope root directory>\groups\master.config** file, and set the value as follows:
  - **=true** to save all runs in the same file with time-stamped run start/stop marker lines.
  - **=false** to backup the file each time a new run is logged.
- 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 Virtual User Generator 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.
- By default, the number of Web Script monitors that can run simultaneously is 20. When this number is exceeded, SiteScope places the rest in a queue to await execution. You can change the number of monitors that can run simultaneously by modifying the **Web Script monitor queue size** in **Preferences > Infrastructure Preferences > Monitor Settings**. The maximum number of Web Script monitors that can run simultaneously is 40. You can also change the amount of time for the monitor to wait in the queue before timing out by modifying the **Web Script monitor queue timeout (seconds)** property. The default queue timeout is 120 seconds.
- The Web Script monitor supports script names with English characters only.
- The Web Script monitor is not available when working in BSM and cannot be configured in System Availability Management. The monitor's data cannot be reported to BSM or HPOM.
- If you are unable to retrieve counters for the Web Script monitor (the JSON output file was not created by the Load Generator during the monitor run), check that the Load Generator is installed and that it has sufficient permissions on the UNIX environment to write to the SiteScope folder.
- To use this monitor with SiteScope Failover, you must install the same version of the Load Generator on the Failover server, and specify the path in **Preferences > Infrastructure Preferences > Custom Settings > loadGeneratorPath**, or add the path to `_loadGeneratorPath=` in the **<SiteScope root>\groups\master.config** file.
- When configuring the monitor, make sure you set a monitor frequency that provides sufficient time for the Load Generator to completely run the web script and generate output. For large web scripts, we recommend using the default monitor frequency (15 minutes).
- If the Duration value for some of the transactions is less than the value for some of the contributing measurements, it might be due to parallel retrieval of different components of the transactions through different sockets. In such cases, add the following expression to your script to prevent opening of multiple sockets:  
`web_set_sockets_option("MAX_CONNECTIONS_PER_HOST", "1")`

# Chapter 111: Web Server Monitor

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. 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 in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Web Server monitor.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	1 OSi license per monitored host

## Tasks

### How to Configure the Web Server Monitor

1. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.
2. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## Web Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	<p>Name of 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>
<b>Browse Servers</b>	<p>Opens the HP SiteScope Discover Servers dialog box, enabling you to 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 How to Configure SiteScope to Monitor a Remote Microsoft Windows Server in the Using SiteScope Guide.</li></ul>
<b>Add Remote Server</b>	<p>Opens the Add Microsoft Windows Remote Server dialog box, enabling you to enter the configuration details. For user interface details, see New/Edit Microsoft Windows Remote Server Dialog Box in the Using SiteScope Guide.</p> <p><b>Note:</b> This button is available for SiteScope running on Windows platforms only.</p>
<b>Web server</b>	<p>Web server type for the selected Web server.</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>

UI Element	Description
<b>Log file path</b>	<p><b>For SiteScope running on Windows platforms:</b> Select the Web Server from the list. If your Web server does not appear in the list, enter the full path to the Web server log file.</p> <p><b>For SiteScope running on UNIX platforms:</b> Enter the full path of 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>Enter the column number which contains the Request Size if your Web server saves information in a custom format.</p> <p>If this item is blank, the common log file format is assumed.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

Measures Web Server Logs

- hits
- bytes
- hits/minute
- bytes/minute

## Tips/Troubleshooting

### General Notes/Limitations

When configuring this monitor in template mode, the **Browse Servers** and **Add Remote Server** buttons are not displayed, and some fields that contain drop-down lists may be displayed as text boxes.

# Chapter 112: Web Service Monitor

The Web Service monitor enables you 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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the Web Service monitor.

## Learn About

This section includes:

- ["Web Service Monitor Overview" below](#)
- ["Supported Platforms/Versions" on the next page](#)
- ["Support for IPv6 Addresses" on the next page](#)
- ["SSL Connectivity" on the next page](#)
- ["Status" on page 786](#)
- ["Integration with Business Service Management for SOA" on page 787](#)
- ["Web Service Topology" on page 787](#)
- ["License Consumption" on page 787](#)

## 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 2003 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/2000/xp/Group/) (<http://www.w3.org/2000/xp/Group/>).

For information about WSDL, refer to the [Microsoft site](http://msdn2.microsoft.com/en-us/library/ms996486.aspx) (<http://msdn2.microsoft.com/en-us/library/ms996486.aspx>).



## Supported Platforms/Versions

The following specification features are currently supported:

- WSDL 1.1, 2.0
- SOAP 1.1, 1.2
- 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:

- WSS (Web Services Security) is currently not supported.
- 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>
```

## Support for IPv6 Addresses

This monitor supports the IPv6 protocol. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings (**Preferences > Infrastructure Preferences > Server Setting**). If this option is selected, whenever a host name is specified for a remote server and the name is resolved to both IPv4 and IPv6, the IPv6 address is used.

When using IPv6, this monitor supports the HTTP protocol.

If specifying a literal IPv6 address as the name for the monitored remote server when IPv6 addressing is enabled, the IP address must be enclosed in square brackets ("[" , "]"). For example:

```
http://[2004:DB8:2a:1005:230:48ff:fe73:982d]:8080
```

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

## SSL Connectivity

Web servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the WSDL URL or Web service server URL.

**Tip:** Usually both of these URLs are used for the same domain—protocol and HTTP port. However, they may differ for complicated or distributed environments. Therefore, you might want to import a certificate for each URL. The Web service server URL can be found in the WSDL.

For example, for SiteScope API WSDL URL is `https://SITE SCOPE_HOST:8443/SiteScope/services/APIConfigurationImpl?wsdl`

This WSDL file contains the following lines:

```
<wsdl:service name="SiteScopeExternalAPI">
<wsdl:port binding="impl:APIConfigurationImplSoapBinding" name="APIConfigurationImpl">
<wsdlsoap:address location="https:// SITESCOPE_
HOST:8443/SiteScope/services/APIConfigurationImpl"/>
</wsdl:port>
</wsdl:service>
```

The Web service server URL is found in the `location` attribute.

If you use a custom value for **Web service server URL** (in the HTTP Settings of the monitor), the certificate should be imported for the domain that was used in this custom 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 the UI Descriptions section below.
- Importing the server certificate. For details on how to perform this task, see ["How to Configure the Web Service Monitor" on the next page](#).

The following cryptographic protocols are supported (on IPv6 and IPv4):

Protocol/HTTP Client used by SiteScope	Java ("Use WinInet" is not selected)	WinInet ("Use WinInet" is selected)
SSLv2	x	x
SSLv3	√	√
TLSv1.0, TLSv1.1, TLSv1.2	√	√

## 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

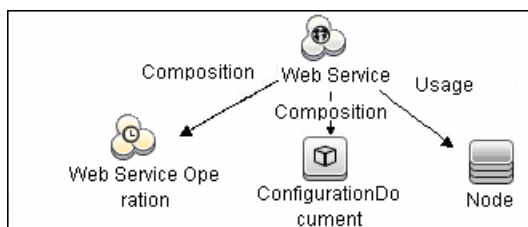
The final status result is either OK, error, or warning based on the threshold established for these conditions.

## Integration with Business Service Management for SOA

If SiteScope is reporting to BSM, the monitor sends SOA samples, in addition to the regular samples it sends, for use in BSM for SOA. If the logging setting in **HP Integration Settings** is set to **Disable reporting metrics to BSM**, the monitor does not send any samples to BSM.

## Web Service Topology

The Web Service monitor can identify the topology of the Web Service being monitored. If **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting), the monitor creates the following topology in BSM's RTSM.



The CIs are created only for the monitored entities according to the counters that you select.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

For information about the SOA topology, see SOA Views and Their Components in the BSM User Guide in the BSM Help.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per monitor	One URL license per monitored URL

## Tasks

This section includes:

- ["How to Configure the Web Service Monitor" below](#)
- ["How to Manually Import Server Certificates " on the next page](#)

### How to Configure the Web Service Monitor

1. Configure the monitor properties
  - a. Make sure you have the user permissions and credentials on the remote server that you want to monitor as specified in Permissions and Credentials.

- b. Configure the monitor properties as required. For a description of each setting, see the UI Descriptions section below.
2. Import the server certificates (if the Web Server is configured to use SSL encryption)  
If the WSDL URL or Web service server URL 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 [How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide](#).
  - Import the server certificates manually. For details, see ["How to Manually Import Server Certificates" below](#).
3. Enable topology reporting - optional  
To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see ["Web Service Topology" on the previous page](#).  
For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

**Tip:** The **Web Service Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see Web Service Tool in the Using SiteScope Guide.

## How to Manually Import Server Certificates

Instead of using Certificate Management, you can manually import certificates 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 in the Using SiteScope Guide.

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.

# UI Descriptions

## Web Service Monitor Settings

User interface elements are described below:

UI Element	Description
<b>WSDL Settings</b>	
<b>WSDL location</b>	Select one of the following options: <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> Your WSDL files must have the extension .wsdl.
<b>Get Data</b>	Retrieves the specified WSDL file and analyzes it for method arguments. The ensuing page displays the measurements available for monitoring.
<b>Service name</b>	Name of the service to be invoked. During initial setup, this is extracted from the WSDL file.
<b>Port name</b>	Name of the port to be invoked. During initial setup, this is extracted from the WSDL file.
<b>Method name</b>	Name of the method to be invoked. During initial setup, this is extracted from the WSDL file.
<b>Method name space</b>	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>	XML name space for the schema in the SOAP request.
<b>SOAP action</b>	SOAP action URL in the header of the SOAP request to the Web Service.

UI Element	Description
<b>Name of arguments</b>	<p>Displays 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) =</p> <p>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>	Uses the XML in the <b>User SOAP XML</b> box. This enables you to use XML that has been manually defined.
<b>Use Text</b>	Select this option if you want to use the XML displayed in the text area.
<b>User 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>Use File</b>	Select this option to use the XML file defined in the templates.soap folder.
<b>Soap XML File</b>	<p>Select the XML file from the drop-down list.</p> <p>Note: You must manually place the XML file in the templates.soap folder.</p>
<b>Reload XML files</b>	Refreshes the current list of files in the drop-down list.
<b>Main Settings</b>	

UI Element	Description
<b>Timeout (seconds)</b>	Amount of 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 if the Web service is based on Microsoft .NET.
<b>Content match</b>	<p>Text string to check for in the returned page or frameset. If the text is not contained in the page, the monitor displays the message <code>no match on content</code>.</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 <code>i</code> 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></p> <ul style="list-style-type: none"> <li>The search is case sensitive.</li> <li>Content match behavior was changed for the Web Service monitor in SiteScope 10.12. To enable Web Service monitors defined prior to SiteScope 10.12 to match the correct value, the <b>Web Service Monitor use common content match</b> setting must be selected in <b>Preferences &gt; Infrastructure Preferences &gt; Monitor Settings</b>.</li> </ul>
<b>HTTP Settings</b>	
<b>Web service server URL</b>	Displays the URL of the Web service server to be monitored.
<b>HTTP user agent</b>	HTTP user agent for the SOAP request.
<b>HTTP content type</b>	Content type of the HTTP request.
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	Domain name and port of an HTTP Proxy Server if a proxy server can be used to access the URL.
<b>Proxy server user name</b>	Proxy server user name if required to access the URL. <b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.
<b>Proxy server password</b>	Proxy server password if required to access the URL. <b>Note:</b> Your proxy server must support Proxy-Authentication for these options to function.

UI Element	Description
<b>Authentication 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>	<p>Authorization user name if the web service requires a user name and password for access (Basic, Digest, or NTLM authentication).</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>
<b>Authorization password</b>	<p>Authorization password if the web service requires a user name and password for access (Basic, Digest, or NTLM authentication).</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>
<b>Client side certificate</b>	<p>If you need to use a client side certificate to access the WSDL URL or Web service server URL, select the certificate file using the drop down menu. Client side certificate files must be copied into the <b>&lt;SiteScope root&gt;\templates.certificates</b> directory. Normally, this is a (.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>
<b>Client side certificate password</b>	<p>Password if you are using a client side certificate and that certificate requires a password.</p> <p><b>Default value:</b> Empty</p>
<b>Accept untrusted certificates for HTTPS</b>	<p>If you are accessing a WSDL URL or Web service server 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 <a href="#">"SSL Connectivity" on page 785</a>.</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 WSDL URL or Web service server 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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.



## Tips/Troubleshooting

### General Notes/Tips

When setting the **round trip time** counter in Threshold Settings, the counter value is in seconds; for all other monitors, it is in milliseconds. This counter is also measured and displayed in the SiteScope Dashboard in seconds.

# Chapter 113: WebLogic Application Server Monitor

The WebLogic Application Server monitor enables you to monitor the statistics of WebLogic Application Servers version 6 through 8. To monitor WebLogic Application Server 11g (10.3.1-10.3.5) or 12c, use a JMX or Dynamic JMX monitor as described in ["JMX Monitor" on page 323](#) and ["Dynamic JMX Monitor" on page 236](#).

**Tip:** 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 Templates.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the WebLogic Application Server monitor.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host Note: Monitor is not available when using Community edition.

## Learn About

### 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.

The 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:

- WebLogic Application Server Monitors cannot be used to monitor WebLogic 11g (10.3.1-10.3.5) or 12c servers. To monitor these servers, use a JMX or Dynamic JMX monitor as described in ["JMX Monitor" on page 323](#) and ["Dynamic JMX Monitor" on page 236](#).  
Monitoring WebLogic 9.x and 10.x is no longer supported due to different Java versions run by SiteScope 11.2x and WebLogic Application Server 9.x and 10.x.
- 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 BSM. For details, see ["WebLogic Application Server Topology" on page 326](#).

- SiteScope also provides a solution template that includes a set of predefined monitors to create a monitoring solution for various aspects of a WebLogic Application Server. For details, see WebLogic Solution Templates in the Using SiteScope Guide.

## Tasks

### How to Configure the WebLogic Application Server Monitor

#### 1. Prerequisites

Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.

#### 2. 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.

#### 3. 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.

#### 4. Configure SiteScope to use T3 over SSL against a WebLogic 7.x or 8.x server - optional

Perform the following steps to configure a WebLogic monitor with the **Secure Server** option to monitor a WebLogic 7.x or 8.x server.

- 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.
- 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
```
- Obtain a valid Oracle license file and put it somewhere on the SiteScope machine. This is the file named **license.bea** in the BEA installation directory.
- 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>\javalib\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 Oracle 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.

## 5. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## WebLogic Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Authentication Settings</b>	
<b>Target</b>	Name of the server where WebLogic is running.
<b>Server</b>	Address of the server where WebLogic is running.
<b>Port number</b>	Port number that the WebLogic server is responding on. <b>Default value:</b> 7001
<b>User name</b>	User name required to log on to the WebLogic server.
<b>Password</b>	Password required to log on to the WebLogic server.
<b>Secure server</b>	Select if 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

UI Element	Description
<b>Advanced Settings</b>	
<b>WLCipher jar file</b>	<p>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.</p> <p>Enter the absolute path to the file on the SiteScope machine.</p> <p><b>Example:</b> C:\bea\weblogic81\server\lib\wlcipher.jar</p> <p><b>Note:</b> This option is for use only with the Secure Server (SSL) option.</p>
<b>WebLogic license file</b>	<p>Enables the Secure Server (SSL) option. Enter the absolute path to the Oracle license file that was copied to the SiteScope machine.</p> <p><b>Example:</b> C:\bea\license.bea</p>
<b>JVM</b>	<p>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:\j2sdk1.4.1\jre\bin\javaw.exe</p>
<b>WebLogic jar file</b>	<p>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>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>
<b>Timeout (seconds)</b>	<p>Amount of time, in seconds, to 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>Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.</p>

UI Element	Description
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" on the next page</a>.</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>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is a list of counters that can be configured for this monitor (the counters listed are examples and the list is not comprehensive, since counters vary depending on what application is installed).

<p><b>Log Broadcaster Runtime</b></p> <ul style="list-style-type: none"> <li>• MessagesLogged</li> </ul> <p><b>Server Runtime</b></p> <ul style="list-style-type: none"> <li>• ConnectionPoolCurrentCount</li> <li>• ConnectionPoolsTotalCount</li> <li>• Connector Service Runtime</li> <li>• Execute Queue Runtime</li> <li>•</li> <li>ExecuteThreadCurrentIdleCount</li> <li>• PendingRequestCurrentCount</li> <li>• PendingRequestOldestTime</li> <li>• ServicedRequestTotalCount</li> </ul> <p><b>JMS Runtime</b></p> <ul style="list-style-type: none"> <li>• ConnectionsCurrentCount</li> <li>• JMSServersCurrentCount</li> <li>• JMSServersHighCount</li> <li>• JMSServersTotalCount</li> <li>• ConnectionsHighCount</li> <li>• ConnectionsTotalCount</li> </ul> <p><b>JTA Runtime</b></p> <ul style="list-style-type: none"> <li>• SecondsActiveTotalCount</li> <li>• TransactionRolledBackTotal Count</li> <li>• TransactionHeuristicsTotal Count</li> <li>• TransactionRolledBackSystem Total Count</li> <li>• TransactionRolledBackApp Total Count</li> <li>• TransactionAbandoned TotalCount</li> <li>• TransactionTotalCount</li> <li>• TransactionRolledBack Timeout TotalCount</li> <li>• ActiveTransactionsTotal Count</li> </ul>	<ul style="list-style-type: none"> <li>• TransactionCommitted TotalCount</li> <li>• TransactionRolled Back Resource TotalCount</li> </ul> <p><b>JVM Runtime</b></p> <ul style="list-style-type: none"> <li>• HeapFreeCurrent</li> <li>• HeapSizeCurrent</li> </ul> <p><b>Time Service Runtime:Time Event Generator</b></p> <ul style="list-style-type: none"> <li>• ExceptionCount</li> <li>• ExecutionsPerMinute</li> <li>• ExecutionCount</li> <li>• ScheduledTriggerCount</li> </ul> <p><b>WLEC Connection Service Runtime</b></p> <ul style="list-style-type: none"> <li>• ConnectionPoolCount</li> </ul> <p><b>Web App Component Runtime</b></p> <ul style="list-style-type: none"> <li>• Activation Time</li> <li>• Admin Server Listen Port</li> <li>• Listen Port</li> <li>• Open Sessions Current Count</li> <li>• Open Sessions HighCount</li> </ul>	<ul style="list-style-type: none"> <li>• Open Sockets Current Count</li> <li>• Restarts Total Count</li> <li>• Sessions Opened Total Count</li> <li>• Sockets Opened Total Count</li> </ul> <p><b>Servlet Runtime (includes ability to monitor JSPs, classes, HTTP client information, etc.)</b></p> <ul style="list-style-type: none"> <li>• PoolMaxCapacity</li> <li>• ExecutionTimeLow</li> <li>• ReloadTotalCount</li> <li>• ExecutionTimeHigh</li> <li>• ExecutionTimeTotal</li> <li>• InvocationTotalCount</li> <li>• ExecutionTime Average</li> </ul> <p><b>Server Security Runtime</b></p> <ul style="list-style-type: none"> <li>• InvalidLoginAttempts TotalCount</li> <li>• InvalidLoginUsersHigh Count</li> <li>• LockedUsersCurrent Count</li> <li>• LoginAttemptsWhile Locked TotalCount</li> <li>• UnlockedUsersTotal Count</li> <li>• UserLockoutTotal Count</li> </ul>
--	--	---

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 114: WebSphere Application Server Monitor

The WebSphere Application Server monitor enables you to monitor the availability and server statistics of WebSphere Application Servers. This enables you to watch server loading for performance, availability, and capacity planning.

Create a separate WebSphere Application Server monitor instance for each WebSphere 5.x, 7.0x, 8.0x and 8.5x 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.

**Tip:** 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 Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the WebSphere Application Server monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["WebSphere Application Server Topology" below](#)
- ["License Consumption" on the next page](#)

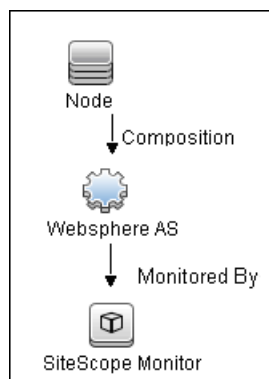
### Supported Platforms/Versions

This monitor supports monitoring server performance statistics from WebSphere 5.x, 6.0x, 6.1x, 7.0x, 8.0x, and 8.5x servers.

### WebSphere Application Server Topology

The WebSphere Application Server monitor can identify the topology of the WebSphere Application Servers being monitored. The monitor creates the following topology in BSM's RTSM.





For details on enabling topology reporting, see the task below.

For information about retrieving topologies and reporting them to BSM, see Reporting Discovered Topologies to BSM in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host
	Note: Monitor is not available when using Community edition.

## Tasks

This section includes:

- ["How to Configure the WebSphere 5.x Application Server Monitoring Environment" below](#)
- ["How to Configure the WebSphere 6.0x Application Server Monitoring Environment" on the next page](#)
- ["How to Configure the WebSphere 6.1x Application Server Monitoring Environment" on page 806](#)
- ["How to Configure the WebSphere 7.0x, 8.0x or 8.5x Application Server Monitoring Environment" on page 811](#)

### How to Configure the WebSphere 5.x Application Server Monitoring Environment

#### 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.

**Caution:** 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 in the previous step.

- 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

Configure the WebSphere Application Server monitor settings as required.

For monitor user interface details, see "[WebSphere Application Server Monitor Settings](#)" on page 817.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting). For details on the monitor topology, see "[WebSphere Application Server Topology](#)" on page 800.

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

## How to Configure the WebSphere 6.0x Application Server Monitoring Environment

1. 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 "[How to Configure the WebSphere 6.0x Server Environment Using Internal Java](#)" on the next page.
  - For details on configuring the WebSphere 6.0x monitoring environment using external Java, see "[How to Configure the WebSphere 6.0x Server Environment Using External Java](#)" on page 805.

**Tip:** We recommend using internal Java for each WebSphere monitor because it reduces system

load and increases SiteScope performance. When using external java, SiteScope creates a new java process for each monitor taking up to 254 MB of memory per monitor. It is also takes longer to create an external process and connect it.

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 user interface details, see ["WebSphere Application Server Monitor Settings" on page 817](#).

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

4. Monitor different instances simultaneously - Optional

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 ["How to Configure the WebSphere 6.1x Application Server Monitoring Environment" on page 806](#).

How to Configure the WebSphere 6.0x Server Environment Using Internal Java

- a. Before configuring WebSphere Application Server monitors, merge all \*.jks keystores and truststores from all WebSphere servers you are going to monitor to a single keystore and truststore vault, and use this in all WebSphere Application Server monitor configurations.

This is a workaround to an IBM issue which is reproduced on all supported WebSphere versions: a remote client cannot access different application servers using different jks files even when the client code has provisions to use different jks file for each server (<http://www-01.ibm.com/support/docview.wss?uid=swg1PK28771>).

- b. 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% (replace all appearances of %WAS\_ENV% and %SIS\_HOME% with the actual value).
- c. 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 (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\WebSphere\AppServer\java\jre\lib\ext\ibmjceprovider.jar	%WAS_ENV%\ibmjceprovider.jar (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\WebSphere\AppServer\profiles\ <ServerName>\etc\ DummyClientTrustFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named <b>default</b> )	%WAS_ENV%\
<WAS_SERVER>\WebSphere\AppServer\profiles\ <ServerName>\etc\DummyClientKeyFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named <b>default</b> )	%WAS_ENV%\

- d. (SSL only) Import the SSL server certificates. You can use Certificate Management to import the certificates, or you can import the certificates manually.
  - o For details on importing certificates using Certificate Management, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
  - o For details on importing certificates manually, see "[How to manually import server certificates for WebSphere 6.0x](#)" on the next page.

**Note:** Make sure you enter the WebSphere SOAP port which you specify in the WebSphere Application Server Monitor Settings.

- e. After importing the server certificates, restart the SiteScope server.

- f. Continue with step 2 of "How to Configure the WebSphere 6.0x Application Server Monitoring Environment" on page 802.

## How to Configure the WebSphere 6.0x Server Environment Using External Java

- a. Before configuring WebSphere Application Server monitors, merge all \*.jks keystores and truststores from all WebSphere servers you are going to monitor to a single keystore and truststore vault, and use this in all WebSphere Application Server monitor configurations.

This is a workaround to an IBM issue which is reproduced on all supported WebSphere versions: a remote client cannot access different application servers using different jks files even when the client code has provisions to use different jks file for each server (<http://www-01.ibm.com/support/docview.wss?uid=swg1PK28771>).

- b. 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 this 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, you can prepare the WebSphere environment for monitoring WebSphere 6.x.

- c. On the WebSphere server, select **Servers > Application Servers > <server name> > Performance Monitoring Infrastructure (PMI)** and make sure that the counters are set to **Extended**.
- d. 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.

- e. Continue with step 2 of "How to Configure the WebSphere 6.0x Application Server Monitoring Environment" on page 802.

## How to manually import server certificates 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 in the Using SiteScope Guide.

- a. Using Internet Explorer 6 or 7, export the SSL certificate to **%WAS\_ENV%\was\_certificate.cert** (in base-64 format).
  - i. 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).
  - ii. In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
  - iii. In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- b. 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**.
- c. Continue with step d of ["How to Configure the WebSphere 6.0x Server Environment Using Internal Java" on page 803](#).

## How to Configure the WebSphere 6.1x Application Server Monitoring Environment

1. 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 ["How to Configure the WebSphere 6.1x Server Environment Using Internal Java" on the next page](#).
  - For details on configuring the WebSphere 6.1x monitoring environment using external Java, see ["How to Configure the WebSphere 6.1x Server Environment Using External Java" on page 809](#).

**Tip:** We recommend using internal Java for each WebSphere monitor because it reduces system load and increases SiteScope performance. When using external java, SiteScope creates a new java process for each monitor taking up to 254 MB of memory per monitor. It is also takes longer to create an external process and connect it.

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:**

- o 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.
- o You can use certificates added using Certificate Management only if **Launch an external JVM** is not selected.
- o When using SSL, you also need to define the **User name** and **Password** to access the WebSphere Application Server.

For user interface details, see the UI Descriptions section below.

### 3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

### 4. Monitor different instances simultaneously - Optional

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.

## How to Configure the WebSphere 6.1x Server Environment Using Internal Java

- a. Before configuring WebSphere Application Server monitors, merge all \*.jks keystores and truststores from all WebSphere servers you are going to monitor to a single keystore and truststore vault, and use this in all WebSphere Application Server monitor configurations.

This is a workaround to an IBM issue which is reproduced on all supported WebSphere versions: a remote client cannot access different application servers using different jks files even when the client code has provisions to use different jks file for each server (<http://www-01.ibm.com/support/docview.wss?uid=swg1PK28771>).

- b. 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% (replace all appearances of %WAS\_ENV% and %SIS\_HOME% with the actual value).
- c. 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 (jar name must be exactly as listed here; rename it if it has a different name)
<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 (jar name must be exactly as listed here; rename it if it has a different name)

From WebSphere Application Server:	To SiteScope machine:
<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 (where <ServerName> is the name of monitored WAS server and not the folder named <b>default</b> )	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\profiles\<ServerName>\ etc\DummyClientKeyFile.jks (where <ServerName> is the name of monitored WAS server and not the folder named <b>default</b> )	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\java\jre\lib\ext\ ibmkeycert.jar	%SIS_HOME%\java\lib\ext

- d. (SSL only) Import the SSL server certificates. You can use Certificate Management to import the certificates, or you can import the certificates manually.

**Note:** Make sure you enter the WebSphere SOAP port which you specify in the WebSphere Application Server Monitor Settings.

- o For details on importing certificates using Certificate Management, see How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide.
  - o For details on importing certificates manually, see ["How to manually import server certificates for WebSphere 6.1x" on page 810](#).
- e. (SSL only) After importing the server certificates, modify the **%SIS\_HOME%\java\lib\security\java.security** file as follows:
- i. Change it so that it reads:

```
# Default JSSE socket factories

ssl.SocketFactory.provider=com.sun.net.ssl.internal.ssl.SSLSocketFactoryI
mpl

ssl.ServerSocketFactory.provider=com.sun.net.ssl.internal.ssl.SSLServerSo
cketFactoryImpl
```

- ii. Add the following additional provider to the list of providers, where N is the number of the next provider in the list:

```
## List of providers and their preference orders (see above):
#
```



```
<all existing providers>
security.provider.N=com.ibm.crypto.provider.IBMJCE
```

- f. Restart the SiteScope server.
- g. Continue with step 2 of "How to Configure the WebSphere 6.1x Application Server Monitoring Environment" on page 806.

## How to Configure the WebSphere 6.1x Server Environment Using External Java

- a. Before configuring WebSphere Application Server monitors, merge all \*.jks keystores and truststores from all WebSphere servers you are going to monitor to a single keystore and truststore vault, and use this in all WebSphere Application Server monitor configurations.

This is a workaround to an IBM issue which is reproduced on all supported WebSphere versions: a remote client cannot access different application servers using different jks files even when the client code has provisions to use different jks file for each server (<http://www-01.ibm.com/support/docview.wss?uid=swg1PK28771>).

- b. 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% (replace all appearances of %WAS\_ENV% with the actual value).
- c. 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  (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\plugins\ com.ibm.ws.runtime_6.1.0.jar	%WAS_ENV%\com.ibm.ws. runtime_6.1.0.jar  (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\WebSphere\ AppServer\profiles\<ServerName>\ etc\DummyClientTrustFile.jks  (where <ServerName> is the name of monitored WAS server and not the folder named <b>default</b> )	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\profiles\<ServerName>\ etc\DummyClientKeyFile.jks  (where <ServerName> is the name of monitored WAS server and not the folder named <b>default</b> )	%WAS_ENV%\

- d. (SSL only) Using Internet Explorer 6 or 7, export the SSL certificate to %WAS\_ENV%\was\_

**certificate.cert** (in base-64 format).

- i. 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).
  - ii. In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
  - iii. In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- e. (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**.

- f. (SSL only) 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
```

- g. Restart the SiteScope machine.
- h. Continue with step 2 of ["How to Configure the WebSphere 6.1x Application Server Monitoring Environment" on page 806](#).

## How to manually import server certificates 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 Overview in the Using SiteScope Guide.

- a. Using Internet Explorer 6 or 7, export the SSL certificate to **%WAS\_ENV%\was\_certificate.cert** (in base-64 format).
  - i. 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).
  - ii. In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
  - iii. In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- b. 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**.

- c. Continue with step d of ["How to Configure the WebSphere 6.1x Server Environment Using Internal Java" on page 807](#).

## How to Configure the WebSphere 7.0x, 8.0x or 8.5x Application Server Monitoring Environment

1. Configure the WebSphere server environment

Configure the WebSphere monitoring environment according to whether you are using internal or external Java.

- For configuring the monitoring environment using internal Java, see ["How to Configure the WebSphere 7.0x, 8.0x or 8.5x Server Environment Using Internal Java" on the next page](#).
- For configuring the monitoring environment using external Java, see ["How to Configure the WebSphere 7.0x, 8.0x or 8.5x Server Environment Using External Java" on page 814](#).

**Tip:** We recommend using internal Java for each WebSphere monitor because it reduces system load and increases SiteScope performance. When using external java, SiteScope creates a new java process for each monitor taking up to 254 MB of memory per monitor. It is also takes longer to create an external process and connect it.

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 user interface details, see "[WebSphere Application Server Monitor Settings](#)" on page 817.

3. Enable topology reporting - optional

To enable topology reporting, make sure that **Report monitor and related CI topology** is selected in **HP Integration Settings** (the default setting).

For user interface details, see "BSM Integration Data and Topology Settings" in the Using SiteScope Guide.

## How to Configure the WebSphere 7.0x, 8.0x or 8.5x Server Environment Using Internal Java

- a. Before configuring WebSphere Application Server monitors, merge all \*.jks keystores and truststores from all WebSphere servers you are going to monitor to a single keystore and truststore vault, and use this in all WebSphere Application Server monitor configurations.

This is a workaround to an IBM issue which is reproduced on all supported WebSphere versions: a remote client cannot access different application servers using different jks files even when the client code has provisions to use different jks file for each server (<http://www-01.ibm.com/support/docview.wss?uid=swg1PK28771>).

- b. 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% (replace all appearances of %WAS\_ENV% and %SIS\_HOME% with the actual value).
- c. 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  (jar name must be exactly as listed here; rename it if it has a different name)

From WebSphere Application Server:	To SiteScope machine:
<code>&lt;WAS_SERVER&gt;\WebSphere\ AppServer\runtimes\ com.ibm.ws.admin.client_7.0.0.jar (for WebSphere 7.0x) or com.ibm.ws.admin.client_8.0.0.jar (for WebSphere 8.0x) or com.ibm.ws.admin.client_8.5.0.jar (for WebSphere 8.5x)</code>	<code>%WAS_ENV%\ com.ibm.ws.admin.client_ 7.0.0.jar or com.ibm.ws.admin.client_ 8.0.0.jar or com.ibm.ws.admin.client_ 8.5.0.jar</code> (jar name must be exactly as listed here; rename it if it has a different name)
<code>&lt;WAS_SERVER&gt;\WebSphere\ AppServer\plugins\ com.ibm.ws.runtime.jar</code>	<code>%WAS_ENV%\ com.ibm.ws.runtime.jar</code>
<code>&lt;WAS_SERVER&gt;\WebSphere\ AppServer\profiles\&lt;ServerName&gt;\etc\DummyClientTrustFile.jks</code> (where <ServerName> is the name of monitored WAS server and not the folder named <b>default</b> )	<code>%WAS_ENV%\</code>
<code>&lt;WAS_SERVER&gt;\WebSphere\ AppServer\profiles\&lt;ServerName&gt;\etc\DummyClientKeyFile.jks</code> (where <ServerName> is the name of monitored WAS server and not the folder named <b>default</b> )	<code>%WAS_ENV%\</code>
<code>&lt;WAS_SERVER&gt;\WebSphere\ AppServer\java\jre\lib\ext\ ibmkeycert.jar</code>	<code>%SIS_HOME%\java\lib\ext</code>
<code>&lt;WAS_SERVER&gt;\WebSphere\ AppServer\java\jre\lib\ibmorb.jar (for WebSphere 8.0x or 8.5x only)</code>	<code>%WAS_ENV%\</code>

- d. (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 [How to Import Server Certificates Using Certificate Management in the Using SiteScope Guide](#).
  - For details on importing certificates manually, see ["How to manually import server certificates for WebSphere 7.0x, 8.0x or 8.5x" on page 816](#).

**Note:** Make sure you enter the WebSphere SOAP port which you specify in the WebSphere Application Server Monitor Settings.

- e. After importing the server certificates, modify the `%SIS_HOME%\java\lib\security\java.security` file as follows:

- i. Change it so that it reads:

```
# Default JSSE socket factories
ssl.SocketFactory.provider=sun.security.ssl.SSLSocketFactoryImpl

ssl.ServerSocketFactory.provider=sun.security.ssl.SSLServerSocketFactoryImpl
```

- ii. Add the following additional provider to the list of providers, where N is the number of the next provider in the list:

```
## List of providers and their preference orders (see above):
#
<all existing providers>
security.provider.N=com.ibm.crypto.provider.IBMJCE
```

- f. Restart the SiteScope server.
- g. Continue with step 2 of "How to Configure the WebSphere 7.0x, 8.0x or 8.5x Application Server Monitoring Environment" on page 811.

## How to Configure the WebSphere 7.0x, 8.0x or 8.5x Server Environment Using External Java

- a. Before configuring WebSphere Application Server monitors, merge all \*.jks keystores and truststores from all WebSphere servers you are going to monitor to a single keystore and truststore vault, and use this in all WebSphere Application Server monitor configurations.

This is a workaround to an IBM issue which is reproduced on all supported WebSphere versions: a remote client cannot access different application servers using different jks files even when the client code has provisions to use different jks file for each server (<http://www-01.ibm.com/support/docview.wss?uid=swg1PK28771>).

- b. 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% (replace all appearances of %WAS\_ENV% with the actual value).
- c. 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\**\*.*

From WebSphere Application Server:	To SiteScope machine:
<WAS_SERVER>\runtimes\ com.ibm.ws.admin.client_7.0.0.jar (for WebSphere 7.0x) or com.ibm.ws.admin.client_8.0.0.jar (for WebSphere 8.0x) or com.ibm.ws.admin.client_8.5.0.jar (for WebSphere 8.5x)	%WAS_ ENV%\com.ibm.ws.admin.clien t_7.0.0.jar or %WAS_ ENV%\com.ibm.ws.admin.clien t_8.0.0.jar or %WAS_ ENV%\com.ibm.ws.admin.clien t_8.5.0.jar  (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\plugins\com.ibm.ws.runtime.jar	%WAS_ ENV%\com.ibm.ws.runtime.jar  (jar name must be exactly as listed here; rename it if it has a different name)
<WAS_SERVER>\WebSphere\ AppServer\profiles\<ServerName>\etc\DummyClientTrustFile .jks  (where <ServerName> is the name of monitored WAS server and not the folder named <b>default</b> )	%WAS_ENV%\
<WAS_SERVER>\WebSphere\ AppServer\profiles\<ServerName>\etc\DummyClientKeyFile.j ks  (where <ServerName> is the name of monitored WAS server and not the folder named <b>default</b> )	%WAS_ENV%\
<WAS_SERVER>\WebSphere \AppServer\java\jre\lib\ibmorb.jar (for WebSphere 8.0x or 8.5x only)	%WAS_ENV%\

- d. (SSL only) Using Internet Explorer 6 or 7, export the SSL certificate to **%WAS\_ENV%\was\_certificate.cert** (in base-64 format).
  - i. 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).
  - ii. In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
  - iii. In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- e. (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`.

- f. 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.SSLServer  
SocketFactory  
==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.SSLServer  
SocketFactory
```

- g. Restart the SiteScope machine.
- h. Continue with step 2 of ["How to Configure the WebSphere 7.0x, 8.0x or 8.5x Application Server Monitoring Environment" on page 811](#).

## How to manually import server certificates for WebSphere 7.0x, 8.0x or 8.5x

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 Overview](#) in the [Using SiteScope Guide](#).

- a. Using Internet Explorer 6 or 7, export the SSL certificate to `%WAS_ENV%\was_certificate.cert` (in base-64 format).
- 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).
  - In the Certificate dialog box, select the **Details** tab, and click **Copy to File**.
  - In the Certificate Export Wizard, export the server certificate as **Base-64 encoded X.509 (.CER)** certificate.
- b. 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`.

- c. Continue with step d of ["How to Configure the WebSphere 7.0x, 8.0x or 8.5x Server Environment Using Internal Java"](#) on page 812.

## UI Descriptions

### WebSphere Application Server Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Server</b>	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>Target</b>	Logical name of the server you want to monitor. If this box is left empty, the server name entered above is used.
<b>Launch an external JVM</b>	External JVMs are used for monitoring. 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>	Port number for the SOAP. <b>Default value:</b> 8880
<b>Credentials</b>	User name and password required to access the WebSphere Application Server. Select the option to use for providing credentials: <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 <a href="#">How to Configure Credential Preferences in the Using SiteScope Guide</a>.</li></ul>

UI Element	Description
<b>Version</b>	Version of the WebSphere application you are monitoring (5.x, 6.0x, 6.1x, 7.0x, 8.0x, 8.5x). <b>Default value:</b> 6.1x
<b>WebSphere directory</b>	Path to the WebSphere AppServer directory. <b>Default value:</b> C:\WebSphere\AppServer
<b>Classpath</b>	Additional classpath variables that are to be used by the WebSphere JVM running on the SiteScope machine.
<b>Timeout (seconds)</b>	Amount of 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. <b>Default value:</b> 60 seconds
<b>Trust store</b>	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. <b>Default value:</b> C:\WebSphere\AppServer\profiles\default\etc\DummyClientTrustFile.jks
<b>Trust store password</b>	Password for the SSL trust store file. <b>Default value:</b> WebAS
<b>Key store</b>	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. <b>Default value:</b> C:\WebSphere\AppServer\profiles\default\etc\DummyClientKeyFile.jks
<b>Key store password</b>	Password for the SSL key store file. <b>Default value:</b> WebAS  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: <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> For more information about Key Store passwords, refer to the <a href="http://publib.boulder.ibm.com/infocenter/wasinfo/v4r0/index.jsp?topic=/com.ibm.websphere.v4.doc/wasa_content/050703.html">IBM Information Center</a> ( <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.
<b>Client properties file</b>	Name of the custom client properties file. <b>Default value:</b> soap.client.props (use the default for version 6.x)

UI Element	Description
<b>Security realm</b>	The security realm of the WebSphere application server.
<b>Counters</b>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.
<b>Get Counters</b>	<p>Opens the Select Counters Form, enabling you to select the counters you want to monitor. For the list of counters that can be configured for this monitor, see <a href="#">"Monitor Counters" below</a>.</p> <p><b>Note:</b> There are two types of WebSphere Application Server metrics: Statistics and MBeans. To reduce counter loading time when you click <b>Get Counters</b>, only the Statistics counters are populated; the MBean objects are empty. To get counters for an MBean object, right-click the object, and select <b>Load Counters</b>.</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>Check Configuration</b>	<p>Runs the WebSphere monitor configuration check tool and displays configuration results. This tool provides a step-by-step check of the connection to the server. It checks:</p> <ul style="list-style-type: none"><li>• WebSphere AppClient jars were copied to the SiteScope server.</li><li>• Certificates were imported into the SiteScope java keystore.</li><li>• WebSphere jks files.</li><li>• Secure properties are used (if SSL is enabled).</li></ul>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is a list of counters that can be configured for this monitor (the counters listed are examples and the list is not comprehensive, since counters vary depending on what application is installed).

<p><b>EJBs</b></p> <p>Methods</p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• methodCalls</li> <li>• methodRt (Statistical)</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>Concurrent Actives (Load)</b></p> <ul style="list-style-type: none"> <li>• Current Value</li> <li>• Integral</li> <li>• Mean</li> <li>• Time Since Create</li> </ul> <p><b>Concurrent Lives (Load)</b></p> <ul style="list-style-type: none"> <li>• Current Value</li> <li>• Integral</li> <li>• Mean</li> <li>• Time Since Create</li> </ul> <p><b>Active Methods (Load)</b></p> <ul style="list-style-type: none"> <li>• Current Value</li> <li>• Integral</li> <li>• Mean</li> <li>• Time Since Create</li> </ul> <p><b>Pool Size (Load)</b></p> <ul style="list-style-type: none"> <li>• Current Value</li> <li>• Integral</li> <li>• Mean</li> <li>• Time Since Create</li> </ul> <p><b>Avg Method Rt (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>Avg Create Time (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>Avg Remove Time (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul>	<p><b>Avg Drain Size (Statistical)</b></p> <ul style="list-style-type: none"> <li>• activates</li> <li>• creates</li> <li>• destroys</li> <li>• drainsFromPool</li> <li>• getsFound</li> <li>• getsFromPool</li> <li>• instantiates</li> <li>• loads</li> <li>• Mean</li> <li>• Num</li> <li>• passivates</li> <li>• removes</li> <li>• returnsDiscarded</li> <li>• returnsToPool</li> <li>• stores</li> <li>• Sum of Squares</li> <li>• Total</li> <li>• totalMethodCalls</li> </ul> <p><b>Connection Pools</b></p> <ul style="list-style-type: none"> <li>• Faults</li> <li>• Num Allocates</li> <li>• Num Creates</li> <li>• Num Destroys</li> <li>• Num Returns</li> <li>• Prep Stmt Cache Discards</li> </ul> <p><b>Pool Size (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul> <p><b>Concurrent Waiters (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul> <p><b>Percent Used (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul> <p><b>Percent Maxed (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul>	<p><b>Avg Wait Time (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>JVM Runtime</b></p> <ul style="list-style-type: none"> <li>• freeMemory</li> <li>• totalMemory</li> <li>• usedMemory</li> </ul> <p><b>Servlet Sessions</b></p> <ul style="list-style-type: none"> <li>• Created Sessions</li> <li>• Invalidated Sessions</li> </ul> <p><b>Active Sessions (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul> <p><b>Live Sessions (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul> <p><b>Session Life Time (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>Thread Pools</b></p> <ul style="list-style-type: none"> <li>• Thread Creates</li> <li>• Thread Destroys</li> </ul> <p><b>Active Threads (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul>
---	--	---

<p><b>Pool Size (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul> <p><b>Percent Maxed (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul> <p><b>Transaction Module</b></p> <ul style="list-style-type: none"> <li>• Global Trans Begun</li> <li>• Global Trans Involved</li> <li>• Local Trans Begun</li> <li>• Num Optimization</li> <li>• Global Trans Committed</li> <li>• Local Trans Committed</li> <li>• Global Trans Rolled Back</li> <li>• Local Trans Rolled Back</li> <li>• Global Trans Timeout</li> <li>• Local Trans Timeout</li> </ul> <p><b>Active Global Trans (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul> <p><b>Active Local Trans (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul> <p><b>Global Tran Duration (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>Local Tran Duration (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul>	<p><b>Global Before Completion Duration (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>Global Prepare Duration (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>Global Commit Duration (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>Local Before Completion Duration (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>Local Commit Duration (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>Web App Servlets</b></p> <ul style="list-style-type: none"> <li>• Total Requests</li> <li>• Num Errors</li> <li>• Num Loaded Servlets</li> <li>• Num Reloads</li> </ul> <p><b>Concurrent Requests (Load)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Time Since Create</li> <li>• Integral</li> <li>• Current Value</li> </ul>	<p><b>Response Time (Statistical)</b></p> <ul style="list-style-type: none"> <li>• Mean</li> <li>• Num</li> <li>• Sum of Squares</li> <li>• Total</li> </ul> <p><b>InvokerServlet</b></p> <ul style="list-style-type: none"> <li>• concurrentRequests (Load)</li> <li>• Current Value</li> <li>• Integral</li> <li>• Mean</li> <li>• Num</li> <li>• numErrors</li> <li>• responseTime (Statistical)</li> <li>• Sum of Squares</li> <li>• Time Since Create</li> <li>• Total</li> <li>• totalRequests</li> </ul> <p><b>JSP_1.1_Processor</b></p> <ul style="list-style-type: none"> <li>• concurrentRequests (Load)</li> <li>• Current Value</li> <li>• Integral</li> <li>• Mean</li> <li>• Num</li> <li>• numErrors</li> <li>• responseTime (Statistical)</li> <li>• Sum of Squares</li> <li>• Time Since Create</li> <li>• Total</li> <li>• totalRequests</li> </ul>
--	--	---

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

## Monitor Specific Notes/Limitations

- After installing SiteScope 11.23 on a SiteScope 11.20 environment, SiteScope forces you to reload the counters tree if you want to add new counters to the WebSphere Application Server monitor. Counters that were previously selected are lost, so you need to reselect them if required.
- There are two types of WebSphere Application Server metrics: Statistics and MBeans. To reduce counter loading time when you click **Get Counters**, only the Statistics counters are populated; the MBean objects are empty. To get counters for an MBean object, right-click the object, and select **Load Counters**.
- If you encounter "java.lang.ClassNotFoundException: com.ibm.security.krb5.KrbException" while setting up this monitor for a WebSphere Application Server environment where security is enabled, copy the **ibmjgssprovider.jar** from **<WAS\_SERVER>\WebSphere\AppServer\java\jre\lib\** to **<SiteScope root directory>\java\lib\ext\**, and then restart SiteScope.
- Information about which WebSphere monitor was loaded first, and which certificates it is configured with, are displayed in the logs.

The following appears in the **RunMonitor.log** after enabling debug for the WebSphere Application Server monitor:

```
DEBUG - -----  
DEBUG - FIRST WEBSphere MONITOR RAN UPDATE IS: __SiteScopeRoot__ -  
>UpperGroupName->SubGroupName::MonitorName  
DEBUG - KEYSTORE LOCATION: /PATH/TO/FILE  
DEBUG - TRUSTSTORE LOCATION: /PATH/TO/FILE  
DEBUG - -----
```

# Chapter 115: WebSphere MQ Status Monitor

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. You can set the error and warning thresholds for the WebSphere MQ Status monitor on as many as fifteen function measurements.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the WebSphere MQ Status monitor.

## Learn About

This section includes:

- ["Supported Platforms/Versions" below](#)
- ["Monitoring MQ Events" below](#)
- ["Authentication" on the next page](#)
- ["Channel Status Codes" on the next page](#)
- ["License Consumption" on page 825](#)

## Supported Platforms/Versions

- This monitor supports monitoring on WebSphere MQ (formerly known as MQSeries) Servers 5.2, 5.3, 5.3.1, 6.0, 7.0, 7.0.1, 7.0.1.3, 7.1, 7.1.0.5, 7.5, 8.0, 8.0.0.2, and 8.0.0.4.
- This monitor is indifferent to the platform on which the WebSphere MQ server is installed, whether it is Windows, z/OS, HP-UX, Linux, AIX, or Sun Solaris.

## 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>\javallib\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. We recommend adding the SiteScope user to the server's MQM group. For information about MQ security exits and other authentication schemes, consult the IBM WebSphere MQ documentation.

If the SiteScope user has reduced MQ permissions (is not part of server's MQM group), they can still monitor MQ objects by configuring the MQ server as specified in ["Monitoring MQ Objects with a regular user" on page 829](#).

### 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 HPE 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	n/a	n/a



MQ Channel Status	MQ Coding Scheme	HP Coding Scheme
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.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per instance (that is, channel or queue)	One OSi license per monitored host Note: Monitor is not available when using Community edition.

## Tasks

### How to Configure the WebSphere MQ Status Monitor

1. **Download and install the IBM MQ 8.0 SupportPacs (when monitoring using WebSphere MQ 8.0 libraries)**
  - a. Download the WebSphere MQ V8.0 client from the [IBM Web site \(http://www-01.ibm.com/support/docview.wss?rs=171&uid=swg24037500&loc=en\\_US&cs=utf-8&lang=en\)](http://www-01.ibm.com/support/docview.wss?rs=171&uid=swg24037500&loc=en_US&cs=utf-8&lang=en) and install it on the machine where the SiteScope server is running.  
Follow the instructions for installing the support pack.
  - b. Stop SiteScope.
  - c. Copy the following jars from the installed MQ directory (**IBM\WebSphere MQ\java\lib**) to the **<SiteScope root directory>\java\lib\ext** folder.
    - **com.ibm.mq.commonservices.jar**
    - **com.ibm.mq.headers.jar**
    - **com.ibm.mq.jar**
    - **com.ibm.mq.pcf.jar**
    - **com.ibm.mq.jmqi.jar**

d. Restart SiteScope.

## 2. Download and install the IBM MQ 7.0 SupportPacs (when monitoring using WebSphere MQ 7.0 libraries)

**Note:** Using WebSphere MQ 7.0 libraries, the SiteScope server is able to monitor WebSphere MQ 7.0 and WebSphere MQ 6.0 servers simultaneously.

a. Download the WebSphere MQ V7.0 client from the [IBM Web site \(http://www-01.ibm.com/support/docview.wss?uid=swg24019253\)](http://www-01.ibm.com/support/docview.wss?uid=swg24019253) and install it on the machine where the SiteScope server is running.

Follow the instructions for installing the support pack.

b. Stop SiteScope.

c. Copy the following jars from the installed MQ directory (**IBM\WebSphere MQ\java\lib**) to the **<SiteScope root directory>\java\lib\ext** folder.

- **com.ibm.mq.commonservices.jar**
- **com.ibm.mq.headers.jar**
- **com.ibm.mq.jar**
- **com.ibm.mq.pcf.jar**
- **com.ibm.mq.jmqi.jar**
- **connector.jar**

d. Restart SiteScope.

## 3. Download and install the IBM MQ 6.0 SupportPacs (when monitoring using WebSphere MQ 6.0 libraries)

a. Download the WebSphere ms0b support pack from the [IBM Web site \(http://www-01.ibm.com/support/docview.wss?uid=swg24000668\)](http://www-01.ibm.com/support/docview.wss?uid=swg24000668) and install it on the machine where the SiteScope server is running.

Follow the instructions for installing the support pack.

b. Stop SiteScope.

c. Copy **com.ibm.mq.pcf-6.1.jar** from **ms0b.zip** to the **<SiteScope root directory>\java\lib\ext** folder.

d. Copy the following files from the installed MQ client to the **<SiteScope root directory>\java\lib\ext** folder.

- **com.ibm.mq.jar**
- **connector.jar**

e. Restart SiteScope.

## 4. Use client SSL for the WebSphere MQ server - optional

To use JSSE (Java Secure Socket environment) in the communication between SiteScope and the WebSphere MQ instance, copy the truststore/keystore files to the SiteScope server, and set a path and password to these files in the below properties of the **<SiteScope root directory>\groups\master.config** file. Truststore and keystore can be put in one file.

For example:

```
_websphereMQTrustStore=C:\trustStore.jks  
_websphereMQKeyStore=C:\trustStore.jks  
_websphereMQKeyStorePassword=P@ssw0rd
```

## 5. 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>\javallib\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.

## 6. Configure the monitor properties

Configure the monitor properties as required.



For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## WebSphere MQ Status Monitor Settings

User interface elements are described below:

UI Element	Description
<b>MQ server name</b>	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>	Port number of the target MQ Server. <b>Default value:</b> 1414
<b>Server connection channel</b>	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.

UI Element	Description
<b>Queue manager</b>	Name of the queue manager whose queues or channels are to be monitored.
<b>User name</b>	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>	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) 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.
<b>Cipher suite</b>	The SSL Cipher suite to use to communicate with the queue manager. For more details, see the WebSphere MQ documentation: <a href="http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp?topic=%2Fcom.ibm.mq.csqzaw.doc%2Fuj34740_.htm">http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp?topic=%2Fcom.ibm.mq.csqzaw.doc%2Fuj34740_.htm</a>
<b>Channel status code scheme</b>	Select a reporting schemes for Channel Status Code values, and click <b>Apply</b> . <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 "<a href="#">Channel Status Codes</a>" on page 824.</li> </ul>
<b>Available Measurements</b>	Displays available MQ queue instances and channel instances, and counters to choose from. For the list of counters that can be configured for this monitor, see " <a href="#">Monitor Counters</a> " on the next page.  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.  For the list of counters that can be configured for this monitor, see " <a href="#">Monitor Counters</a> " on the next page.
<b>Selected Measurements</b>	Displays the measurements currently selected for this monitor, and the total number of selected counters.  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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Monitor Counters

Below is the list of counters that can be configured for this monitor:

Queues	Channels
<ul style="list-style-type: none"> <li>• Current Queue Depth</li> <li>• Event: Queue Depth High</li> <li>• Event: Queue Depth Low</li> <li>• Event: Queue Full</li> <li>• Event: Queue Service Interval High</li> <li>• Event: Queue Service Interval Ok</li> <li>• Queue Depth in %</li> <li>• Queue Open Input Count</li> <li>• Queue Open Output Count</li> <li>• Maximum Queue Depth</li> </ul>	<ul style="list-style-type: none"> <li>• Channel Bytes Received</li> <li>• Channel Bytes Sent</li> <li>• Channel Status</li> <li>• Channel Time Between Sends</li> <li>• No. of Channel Buffers Sent</li> <li>• No. of Channel Buffers Received</li> <li>• No. of Channel Messages Transferred</li> <li>• Event: Channel Activated</li> <li>• Event: Channel Not Activated</li> <li>• Event: Channel Started</li> <li>• Event: Channel Stopped</li> <li>• Event: Channel Stopped by User</li> </ul>

## Tips/Troubleshooting

### General Tips/Limitations

If the WebSphere MQ Status Monitor opens a higher number of communication channels to the WebSphere server than is necessary, you can minimize the request count by setting the property `mqMonitorOneRequest` to `=true` in the `<SiteScope root directory>\groups\master.config` file.

### Monitoring MQ Objects with a regular user

To monitor MQ objects with a regular user that has reduced MQ permissions (a SiteScope user that is not part of server's MQM group), configure the following on the MQ server:

1. On the WebSphere MQ server, create a regular user.

For example, for Windows, enter the following in a command prompt: `net user mq_user mq_password /ADD`

2. Grant specific authority over MQ objects to the required user. In a command prompt, enter:

```
setmqaut -m MYQM -t qmgr -p mq_user +connect +inq +dsp
setmqaut -m MYQM -t q -n SYSTEM.DEFAULT.MODEL.QUEUE -p mq_user +inq +get +dsp
setmqaut -m MYQM -t q -n SYSTEM.ADMIN.COMMAND.QUEUE -p mq_user +inq +put
```

where `MYQM` is the name of the WebSphere MQ queue manager.

3. Grant specific permission for gathering data.

- For a specific queue, enter: `setmqaut -m MYQM -t q -n specific_queue_name -p mq_user +inq +get +dsp +browse`
- For all available queues, enter: `setmqaut -m MYQM -n "*" -t q -p mq_user +browse +dsp +get +inq`

4. To gather data about channels, enter: `setmqaut -m MYQM -n "*" -t chl -p mq_user +dsp`

## Error Codes

The following are common errors and ways to resolve them:

### Error 2540 - “Channel not defined remotely”

com.ibm.mq.jmqi.JmqiException: CC=2;RC=2540;AMQ9204: Connection to host 'my.host(port)' rejected.  
[1=com.ibm.mq.jmqi.JmqiException[CC=2;RC=2540;AMQ9520: Channel not defined remotely.  
[2=172.23.61.90(1417),3=client]],3=172.23.61.90(1417),5=RemoteConnection.analyseErrorSegment]

#### Possible Cause 1:

Different queue managers are using the same port.

#### Solution:

1. Check the listener port by using the MQSC command:

```
$ runmqsc QmgrName  
dis listener(*) port
```

You are looking for:

```
LISTENER(LISTENER.TCP) PORT(bla)
```

2. To change the port used by a queue manager, use the MQSC command:

```
alter listener(listener.tcp) trptype(tcp) port(bla)
```

For more details about channel listener, see the WebSphere documentation:

[http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp?topic=%2Fcom.ibm.mq.csqzah.doc%2Fqc10410\\_.htm](http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp?topic=%2Fcom.ibm.mq.csqzah.doc%2Fqc10410_.htm)

#### Possible Cause 2:

The application used a transport type of MQJMS\_TP\_CLIENT\_MQ\_TCPIP without setting a value for the hostname.

**Solution:** Avoid using localhost as a host name.

### Error 2035 – [MQJE001: Completion Code '2', Reason '2035']

You created a new queue manager in MQ 7.1 or 7.5 or later. The default value for the new feature introduced in 7.1, "Channel Authentication Records" (CHLAUTH) is ENABLED. You can see the value by using runmqsc:

```
$ runmqsc QmgrNadis me  
dis qmgr chlauth  
AMQ8408: Display Queue Manager details  
QMNAME(TEST01) CHLAUTH(ENABLED)
```

By default, the following 3 channel authentication records are generated when a new queue manager is created in WebSphere MQ 7.1 or upgraded to 7.1:

```
$ dis chlauth(*)  
AMQ8878: Display channel authentication record details.  
CHLAUTH(SYSTEM.ADMIN.SVRCONN) TYPE(ADDRESSMAP)  
ADDRESS(*) USERSRC(CHANNEL)  
AMQ8878: Display channel authentication record details.  
CHLAUTH(SYSTEM.*) TYPE(ADDRESSMAP)  
ADDRESS(*) USERSRC(NOACCESS)  
AMQ8878: Display channel authentication record details.
```

CHLAUTH(\*) TYPE(BLOCKUSER)  
USERLIST(\*MQADMIN)

The last record blocks all remote channel access to any MQ Administrator. The effect is that non-administrative users can still connect if suitably authorized to do so, but administrative connections and anonymous connections are disallowed regardless of any Object Authority Manager (OAM) authorization settings. This means that new queue managers in WebSphere MQ 7.1 are much more secure by default than in previous versions, but with the trade off that administrative access must be explicitly defined.

**Possible Solution:**

1. Disable CHLAUTH rules.
2. Add Administrator (or another “advanced” user) to the MQM group.
3. Run the WebSphere MQ Service under this user.
4. Type the user credentials in the WebSphere MQ Monitor settings.

For more information, see the WebSphere documentation: <http://www-01.ibm.com/support/docview.wss?uid=swg21577137>

**Note:** You will not be able to receive messages from the remote queue, only from the local queues.

# Chapter 116: WebSphere Performance Servlet Monitor

Use the WebSphere Performance Servlet Monitor to monitor the server performance statistics for WebSphere 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 WebSphere Performance Servlet Monitor instance for each WebSphere Application Server in your environment. The error and warning thresholds for the monitor can be set on one or more performance statistics.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the WebSphere Performance Servlet monitor.

## Learn About

### Supported Platforms/Versions

This monitor supports monitoring 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, 7.0, 7.0.0.19, 7.0.0.21, 8.0, 8.0.0.1, and 8.0.0.2 servers.

### License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One OSi license per monitored host Note: Monitor is not available when using Community edition.

## Tasks

### How to Configure the WebSphere Performance Servlet Monitor

#### 1. Prerequisites

The following are key requirements for using the WebSphere Performance Servlet Monitor:

- Make sure you have the user permissions and credentials required for this monitor as specified in Permissions and Credentials.
- 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`

## 2. Configure the monitor properties

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

# UI Descriptions

## WebSphere Performance Servlet Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>Server</b>	Name of 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>	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>	Port number to the WebSphere server you want to monitor.

UI Element	Description
<b>Servlet URL</b>	<p>URL of the performance servlet.</p> <p>For WebSphere 6.0 and later, you can use either of the following URLs: /wasPerfTool/servlet/perfservlet or /wasPerfTool/servlet/perfservlet?version=5</p> <p>For previous versions of WebSphere, use the following URL only: /wasPerfTool/servlet/perfservlet?version=5</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• Make sure that WebSphere Performance Servlet is deployed on all versions of WebSphere.</li> <li>• If you need to monitor WebSphere with SSL, you may configure it in the WebSphere Security.</li> </ul>
<b>User name</b>	User name if the URL requires authorization.
<b>Password</b>	Password if the URL requires authorization.
<b>Advanced Settings</b>	
<b>Timeout (seconds)</b>	<p>Amount of 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.</p> <p><b>Default value:</b> 60 seconds</p>
<b>Refresh frequency</b>	<p>Time interval at which the WebSphere server should update the metrics that are requested by this monitor.</p> <p>This value should be equal to or less than the <b>Frequency</b> time interval for the monitor in Monitor Run Settings.</p> <p><b>Default value:</b> 10 minutes</p>
<b>Proxy Settings</b>	
<b>HTTP proxy</b>	Name of the proxy server if required.
<b>Proxy user name</b>	<p>Proxy server user name if required to access the server.</p> <p><b>Note:</b> Your proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy password</b>	Proxy server password if required to access the server.
<b>WebSphere Performance Counters</b>	
<b>Counters</b>	Displays the server performance counters selected for this monitor. Use the <b>Get Counters</b> button to select counters.

UI Element	Description
<b>Get Counters</b>	Opens the Select Counters Form, enabling you to 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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

# Chapter 117: XML Metrics Monitor

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.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the XML Metrics monitor.

## Learn About

This section includes:

- ["XML Metrics Monitor Overview" below](#)
- ["XML Requirements" below](#)
- ["License Consumption" on the next page](#)

### 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.

The error and warning thresholds for the monitor can be set on one or more different objects.

### 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 in the Using SiteScope Guide.

## License Consumption

Points-based Usage	Capacity-based Usage
One point per metric	One URL license per monitored URL

# Tasks

## How to Configure the XML Metrics Monitor

Configure the monitor properties as required.

For a description of each setting, see the UI Descriptions section below.

**Tip:** The **XSL Transformation Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see XSL Transformation Tool in the Using SiteScope Guide.

# UI Descriptions

## XML Metrics Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Main Settings</b>	
<b>XML URL</b>	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>	Domain for Windows NT LAN Manager (NTLM) authorization if it is required to access the URL.

UI Element	Description
<b>Pre-emptive authorization</b>	<p>Option for sending Authorization user name and Authorization password if SiteScope requests the target URL:</p> <ul style="list-style-type: none"> <li>• <b>Use global preference.</b> SiteScope uses 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> Sends the user name and password on the first request SiteScope makes for the target URL.</li> </ul> <p><b>Note:</b> If the URL does not require a user name and password, this option may cause the URL to fail.</p> <ul style="list-style-type: none"> <li>• <b>Authenticate if requested.</b> Sends the user name and password on the second request if the server requests a user name and password.</li> </ul> <p><b>Note:</b> If the URL does not require a user name and password, this option may be used.</p> <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>Amount of time, in seconds, to wait for 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>
<b>Authentication Settings</b>	
<b>Authorization user name</b>	Authorization user name to access the URL with the XML content, if required.
<b>Authorization password</b>	Authorization password to access the URL with the XML content, if required.
<b>Proxy server</b>	Host or domain name and port of the proxy server if using a proxy server to access the XML URL.
<b>Proxy server user name</b>	<p>Proxy server user name if you using a proxy server and the proxy requires a name and password to access the target URL.</p> <p><b>Note:</b> The proxy server must support Proxy-Authenticate for these options to function.</p>
<b>Proxy server password</b>	<p>Proxy server password if you using a proxy server and the proxy requires a name and password to access the target URL.</p> <p><b>Note:</b> The proxy server must support Proxy-Authenticate for these options to function.</p>

UI Element	Description
<b>Accept untrusted certificates for HTTPS</b>	Select 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 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
<b>Counter Settings</b>	
<b>Counters</b>	Displays 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>	Opens the Select Counters Form, enabling you to 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.

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Limitations

When deploying this monitor using a template, an error message is displayed if you clear the **Verify monitor properties with remote server** check box in the Deployment Values dialog box.

## Part 3: Integration Monitors (A-Z)

**Note:** Since EMS functionality was moved to BSM Connector, a free HPE application that provides more functionality and coverage of third-party data, not all EMS monitors are available (check the specific monitor for details). HPE recommends using BSM Connector for all new third-party data integrations. Note that BSM Connector works with BSM 9.20 and later only. For details on BSM Connector, see the BSM Application Administration Guide in the BSM Help.



# Chapter 118: HP OM Event Monitor

The HP OM Event Monitor enables you to integrate an existing HPE OpenView installation with BSM by transferring HPOM messages from HPOM Server to an BSM server.

## Note:

- The HP OM Event monitor is not available when SiteScope is connected to BSM version 9.00 or later (unless the monitor was created in an earlier version of SiteScope that was upgraded to SiteScope 11.20). OM events can be forwarded to BSM 9.00 from the HPOM Server, provided you have an Event Management Foundation license and an integration is configured between Operations Manager and BSM.
- This monitor is not available in the user interface when using Community or Load Testing edition.
- This monitor supports English only. It does not support I18N mode.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP OM Event monitor.

## Learn About

This section includes:

- ["HP OM Event Monitor Overview" below](#)
- ["Supported Versions" below](#)
- ["Status" on the next page](#)

## HP OM Event Monitor Overview

The HP OM Event monitor depends on an HP OM Integration Add-on module to collect events from the HPOM Server. The Add-on, when installed on the HP OM Server, listens to events received by the HPOM system and sends them to the HP OM Event Monitor. The HP OM Event Monitor transfers the events to an BSM 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\hplevent.config**, to define the processing of incoming data and to define the output sample forwarded to BSM. Do not modify this configuration file.

## Supported Versions

This monitor supports:

- HPOM 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.
- HPOM versions 9.0 or later when installed on Red Hat Linux.
- HPOM versions 7.5 or later when installed on Windows.

## 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 Troubleshooting/Limitations in the Using SiteScope Guide.

## Tasks

This section includes:

- ["How to Configure the HPOM Integration Add-on \(UNIX Platforms\)" below](#)
- ["How to Configure the HPOM Integration Add-on \(Windows Platforms\)" on page 845](#)

### How to Configure the HPOM Integration Add-on (UNIX Platforms)

The purpose of the HPOM Integration Add-on is to connect to the HPOM message infrastructure, to receive events from the HPOM, and to forward these events to the SiteScope machine.

**Note:** The HPOM Integration Add-on module is platform specific. Modules are provided for all platforms supported by HPOM/UNIX version 8.24.

1. Install the HPOM integration add-on

Installation packages for the various platforms used below is in **<SiteScope root directory>\conf\ems\hp\addon\OVO-BAC.zip** file.

#### On HP-UX 11.11 platforms:

- Log on as superuser to the HPOM Server. Alternatively, use the su command to gain superuser permissions.
- Copy **HPOvOBac-01.00.000-HPUX11.0-release.depot** installation package to **\tmp**.
- Perform the following command:

```
swinstall -s /tmp/HPOvOBac-01.00.000-HPUX11.0-release.depot \*
```

#### On HP-UX 11.23 platforms:

- Log on as superuser to the HPOM Server. Alternatively, use the su command to gain superuser permissions.
- Copy **HPOvOBac-01.00.000-HPUX11.22\_IPF32-release.depot** installation package to **\tmp**.
- Perform the following command:

```
swinstall -s /tmp/HPOvOBac-01.00.000-HPUX11.22_IPF32-release.depot \*
```

**On Solaris 5.7 or later platforms:**

- Log on as user root to the HPOM Server. Alternatively, use the su command to gain super-user permissions.
- Copy **HPOvOBac-01.00.000-SunOS5.7-release.sparc** installation package to **/tmp**.
- Perform the following command:

```
pkgadd -d /tmp/HPOvOBac-01.00.000-SunOS5.7-release.sparc HPOvOBac
```

2. Configure the HPOM integration add-on

Once installed, the HPOM Integration Add-on must be configured on the HPOM Server before it can be used.

- To configure the HPOM Integration Add-on on the HPOM Server, configure the host name or IP address of the SiteScope machine on which the HPOM Event Monitor is installed:

```
ovconfchg -ns opc.bac -set TargetHost <host name>
```

**Note:** 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>

If you change this setting, make sure to update the HP OM Event Monitor.

**Tip:** HPOM Integration Add-on for UNIX provides a function that improves performance of internal message processing. Enabling this function improves the performance of the HPOM Integration Add-on (and other HPOM components, such as the HPOM Java user interface). This function is disabled by default.

- To enable improved HPOM Add-on performance on UNIX feature, on the HPOM Server, perform the following commands:
  - opcsv -stop
  - ovconfchg -ovrg server -ns opc -set OPCMSGM\_USE\_GUI\_THREAD NO\_RPC
  - opcsv -start

3. Tune the HPOM integration add-on

You can tune the HPOM Integration Add-on by running utilities from the command line on the HPOM 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.

Variable Name	Default Value	Description
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 <code>CacheMax</code> , only the most-recently-used messages in <code>CacheKeep</code> are kept in the cache. All others are removed from the cache.
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 HPOM 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 <code>MaxWaitTime</code> .
MaxWaitTime	120	Maximum number of seconds to wait after connection failures before retry. When doubling the wait time after connection failures exceeds <code>MaxWaitTime</code> , the wait time is no longer doubled and <code>MaxWaitTime</code> 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 <code>MaxQueueLen</code> , the oldest entries are removed from the queue.
NodeKeepTime	900	The HPOM Integration Add-on looks up IP addresses from host names. In addition, OM/Windows host names also need to be looked up from the HPOM 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 <code>NodeKeepTime</code> seconds.

Changing any of these variables automatically updates the HPOM Integration Add-on. There is no need to stop and restart the HP OM Integration Add-on process.

#### 4. Start and stop the HPOM integration add-on

The HPOM Integration Add-on must be started after it is installed.

On UNIX platforms, the HPOM Integration Add-on is controlled by OpenView Control Daemon (ovcd). Using the command line tool **ovc** on the HPOM Server, perform the command:

```
ovc -stop <or start> opc2bac
```

If the HPOM 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 HPOM Integration Add-on.

If the HPOM 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 HPOM API libraries, it may be necessary to stop the Integration Add-on before installing HPOM patches, and start it after the patch installation.

5. Remove the HPOM integration add-on files from the HPOM server

If you must remove the HPOM Integration Add-on files from the HPOM Server, perform the following procedure:

**On HP-UX platforms:**

- Log on as superuser.
- Perform the command: `swremove HPOvOInt.HPOVOBAC`

**On Solaris platforms:**

- Log on as superuser.
- Perform the command: `pkgrm HPOvOBac`

6. Support in HPOM cluster installation

The HPOM Integration Add-on is supported in an HPOM cluster environment. You can do the following tasks:

- Install the HPOM Integration Add-on on each cluster node separately.
- Configure the HPOM Integration Add-on on each cluster node separately. All configuration settings on all cluster nodes must be identical.
- Remove the HPOM Integration Add-on from each cluster node separately.

7. View log file messages

The HPOM Integration Add-on writes log messages into the log file `/var/opt/OV/logSystem.txt`.

Log file entries use the process name **opc2bac** for messages logged by the HPOM Integration Add-on.

## How to Configure the HPOM Integration Add-on (Windows Platforms)

The purpose of the HPOM Integration Add-on is to connect to the HPOM message infrastructure, to receive events from the HPOM, and to forward these events to the SiteScope machine.

**Note:**

- The HPOM Integration Add-on module is platform specific. Modules are provided for all platforms supported by OM/Windows version 7.5.
- Added support to install the HPOM Integration Add-on module on a Windows Server R2 64-bit machine from the **OVO-BAC.zip** installation file.

1. Install the HPOM integration add-on

Installation packages for the various platforms used below is in **<SiteScope root directory>\conf\ems\hp\addon\OVO-BAC.zip** file.

- a. Log on as user administrator to the HPOM Server.
- b. Copy **HPOvXpl-03.10.040-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-03.10.040-WinNT4.0-release.msi /qn`
  - `msiexec /I C:\tmp\HPOvOBac-01.00.000-WinNT4.0-release.msi /qn`

2. Configure the HPOM integration add-on

Once installed, the HPOM Integration Add-on must be configured on the HPOM Server before it can be used. To configure the HPOM Integration Add-on on the HPOM Server, 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>
```

**Note:**

- 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>`
- If you change this setting, make sure to update the HP OM Event Monitor.

3. Tune the HPOM integration add-on

You can tune the HPOM Integration Add-on by running utilities from the command line on the HPOM 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.
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.

Variable Name	Default Value	Description
MinWaitTime	15	If the connecting to the SiteScope receiver failed, the HPOM 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 HPOM 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 HPOM integration add-on

The HPOM Integration Add-on runs as a Windows service and must be started after it is installed. To start or stop the HPOM Integration Add-on on Windows platforms:

- On the HPOM Server, click **Start > Settings> Control Panel > Administrative Tools > Services**.
- Select the service **HP OpenView Operations Message Forwarder to BAC**.
- Click **Start** or **Stop**.

#### 5. Remove the HPOM integration add-on files from the HPOM server

If you must remove the HPOM Integration Add-on files from the HPOM Server, perform the following procedure:

- On the HPOM Server, click **Start > Settings > Control Panel > Administrative Tools > Services**.
- 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 HPOM cluster installation

The HPOM Integration Add-on is supported in an HPOM cluster environment. You can do the following tasks:

- Install the HPOM Integration Add-on on each cluster node separately.
  - Configure the HPOM Integration Add-on on each cluster node separately. All configuration settings on all cluster nodes must be identical.
  - Remove the HPOM Integration Add-on from each cluster node separately.
7. View log file messages
- The HPOM Integration Add-on writes log messages into the **System.txt** log file in the **<DataDir>\log** directory, 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.

## UI Descriptions

### HP OM Event Monitor Settings

User interface elements are described below:

UI Element	Description
HPOM Add-on TCP port	TCP port number as configured in the HPOM Integration Add-on. <b>Default value:</b> 9000

### Field Mapping

User interface elements are described below:

UI Element	Description
Field mapping	<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 BSM.</p> <p>Field mapping is not editable while configuring the monitor and we recommend that you use the out-of-the-box integration mapping. If you must customize the field mapping, locate the file in the following location and edit it in your preferred text editor: <b>&lt;SiteScope root directory&gt;\conf\ems\hp\event.config</b>. 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 Field Mapping Data Types in the Using SiteScope Guide.</p>



## Topology Settings

User interface elements are described below:

UI Element	Description
<b>Script</b>	<p>The out-of-the-box integration script that creates a topology in BSM that is based on the collected data 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 BSM'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_hpovo.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 Editing the Topology Script in the Using SiteScope Guide.</p>

## Export to BSM Connector

User interface elements are described below:

UI Element	Description
<b>Export</b>	<p>Enables exporting technology integration monitors from SiteScope and importing them to BSM Connector as policies. This feature is supported on Technology Database Integration, Technology Log File Integration, and Technology Web Service Integration monitors with a metrics, common events, or legacy events field mapping data type only.</p> <p>Select a folder on the client file system in which to save the policy files, and click <b>Open</b> to perform the export process. For task details, see Export EMS Technology Monitors to a BSM Connector Policy in the Using SiteScope Guide.</p> <p>For details on importing policies to BSM Connector, see the BSM Connector online help system (available from the toolbar of the BSM Connector user interface).</p> <p><b>Note:</b> This button is disabled and a warning message is displayed for integration monitors where export is not supported.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Tips/Troubleshooting

### General Notes/Limitations

- The HP OM Event monitor is not available when SiteScope is connected to BSM version 9.00 or later (unless the monitor was created in an earlier version of SiteScope that was upgraded to SiteScope 11.10).

OM events can be forwarded to BSM 9.00 from the HPOM server, provided you have an Event Management Foundation license and an integration is configured per the instructions in the BSM Installation Guide in the BSM Help.

- For script alerts to be sent to Operations Manager when using an OM script, the **Template** setting in Action Type Settings must be changed to **Default** (by default it is set to **Typical**).

# Chapter 119: HP Service Manager Monitor

This monitor enables you to integrate HPE Service Manager incidents with BSM. The incidents in Service Manager are forwarded to BSM as samples by this SiteScope monitor. The samples are used in reporting data to the BSM applications, such as Service Level Management and Service Health.

## Note:

- This monitor is not available in the user interface when using Community or Load Testing edition.
- 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 Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the HP Service Manager monitor.

## Learn About

This section includes:

- ["HP Service Manager Monitor Overview" below](#)
- ["Supported Versions" on the next page](#)

## HP Service Manager Monitor Overview

The HPE Service Manager Monitor enables you to integrate Incident Management data from an HPE ServiceCenter or HPE Service Manager installation with BSM. 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.

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 HPE Service Manager monitor forwards business service-related incidents to BSM 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 HPE 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 HPE Service Manager monitor CI and the business service CI. The monitor integrates the incident data into samples which are forwarded to BSM applications, such as Service Health and Service Level Management.

For more details on the capabilities of the integration, see How to Integrate HP Service Manager with Business Service Management Components in the BSM User Guide in the BSM Help.

For more detailed information on the CIs and related KPIs, see Integration with HP Service Manager in the BSM User Guide in the BSM Help.

## Supported Versions

This monitor supports:

- ServiceCenter 6.2.6
- Service Manager 7.01, 7.02, 7.11 and 9.20 (previously 7.2)

## Tasks

This section includes:

- ["How to Work with the HP Service Manager Integration" below](#)
- ["How to Copy the JAR File" on the next page](#)
- ["How to Create the JAR File" on the next page](#)

### How to Work with the HP Service Manager Integration

#### 1. Prerequisites

Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see How to Configure the Integration Between SiteScope and BSM in the Using SiteScope Guide.

#### 2. Edit clocks and Incident Management configuration files

If any changes were made to the clocks table, the incident management tables in HPE Service Manager, or both, 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 HPE 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.

#### 3. 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 HPE Service Manager 7.0.x using default settings, no additional JAR configurations are required.
- For integrations with HPE Service Manager 7.1 or 9.2 using default settings, you must copy the JAR file to the **WEB-INF\lib** directory and edit the configuration file. For details, see ["How to Copy the JAR File" on the next page](#).
- For any integration with ServiceCenter or HPE Service Manager that does not use the default configuration, you must create the JAR file. For details, see ["How to Create the JAR File" on the next page](#).

**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.

4. Configure an HP Service Manager monitor in SiteScope

You can create this monitor:

- Using the EMS Integrations Administration portal in BSM.
- Directly in SiteScope.

**Tip:** Monitors must be created in a group in the monitor tree. We recommend that you create a special group for the Service Manager integration.

For details on configuring the monitor settings, see "[HP Service Manager Monitor Settings](#)" on the next page.

## How to Copy the JAR File

1. To enable SiteScope to integrate with HP Service Manager 7.1 or 9.2 using default settings, copy the JAR file from **<SiteScope root directory>\conf\ems\peregrine\lib<SM version>** to **<SiteScope root directory>WEB-INF\lib**.
2. 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.

## How to Create the JAR File

This batch file creates and compiles the files needed for the HPE 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>\conffems\peregrine\create-peregrine-jar.bat** file to run the batch.
  - **UNIX:** You must run the **<SiteScope root directory>\conffems\peregrine\create-peregrine-jar.sh** file from the full path in a terminal window.
6. Restart the SiteScope service on the SiteScope machine.

## UI Descriptions

### HP Service Manager Monitor Settings

User interface elements are described below:

UI Element	Description
<b>HP Service Manager Web Service Endpoint</b>	<p>URL for the HPE Service Manager Web Service. Use the following format: <b>&lt;protocol&gt;://&lt;host_name&gt;:&lt;port&gt;/</b> 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: <b>&lt;protocol&gt;://&lt;SM host&gt;:&lt;SM port&gt;/sc62server/PWS/</b></p> <p>The URL syntax when integrating with Service Manager 6.2.6 is: <b>&lt;protocol&gt;://&lt;SM host&gt;:&lt;SM port&gt;/sc61server/PWS/</b></p>
<b>Username</b>	Designated user name created in HPE Service Manager for the purpose of this integration monitor.
<b>Password</b>	Password of the designated user created in HPE Service Manager for the purpose of this integration monitor.
<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 BSM.</p> <p>Field mapping is not editable while configuring the monitor and we recommend that you use the out-of-the-box integration mapping. If you must customize the field mapping, locate the following file: <b>&lt;SiteScope root directory&gt;\conffems\peregrine\ticket.config</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 details on the field mapping script template, see Field Mapping Data Types in the Using SiteScope Guide.</p>

UI Element	Description
<b>Test Script</b>	<p>Tests 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 BSM.</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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>
<b>Synch Flag</b>	<p>Enables 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>
<b>Synch Time</b>	<p>Time from which the monitor retrieves incidents. Enter a value only when <b>Synch Flag</b> is selected.</p>
<b>Incident Management (probsummary table) query</b>	<p>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

User interface elements are described below:

UI Element	Description
<b>Script</b>	<p>The out-of-the-box integration script that creates a topology in BSM that is based on the collected data 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 BSM's applications.</p> <p>We recommend that you use the topology settings as is (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 Editing the Topology Script in the Using SiteScope Guide.</p>
<b>Test Script</b>	<p>Tests the topology script. This test gives you the results of what events are forwarded to BSM 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Export to BSM Connector

User interface elements are described below:

UI Element	Description
<b>Export</b>	<p>Enables exporting technology integration monitors from SiteScope and importing them to BSM Connector as policies. This feature is supported on Technology Database Integration, Technology Log File Integration, and Technology Web Service Integration monitors with a metrics, common events, or legacy events field mapping data type only.</p> <p>Select a folder on the client file system in which to save the policy files, and click <b>Open</b> to perform the export process. For task details, see Export EMS Technology Monitors to a BSM Connector Policy in the Using SiteScope Guide.</p> <p>For details on importing policies to BSM Connector, see the BSM Connector online help system (available from the toolbar of the BSM Connector user interface).</p> <p><b>Note:</b> This button is disabled and a warning message is displayed for integration monitors where export is not supported.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.



# Chapter 120: NetScout Event Monitor

The NetScout Event Monitor monitors alerts received from the NetScout nGenius server and forwards them to BSM.

## Note:

- This monitor is not available in the user interface when using Community or Load Testing edition.
- 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 Templates in the Using SiteScope Guide.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the NetScout Event monitor.

## Learn About

### 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 BSM. 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.

The NetScout Event Monitor forwards alerting instances to BSM 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 BSM applications, such as Service Health and Service Level Management.

**Note:** For information about Integration Monitor logging and troubleshooting, see Troubleshooting/Limitations in the Using SiteScope Guide.

## Tasks

### How to Integrate Data From a NetScout System

The following are the steps necessary to integrate data from a NetScout system and view the NetScout data in a way that is customized to your needs.

#### 1. Prerequisites

The following are important guidelines and requirements for using the NetScout Event Monitor to forward alerts to BSM.

- Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see [How to Configure the Integration Between SiteScope and BSM](#) in the [Using SiteScope Guide](#).
- 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.

- The NetScout Event Monitor must be set to synchronize integration monitor data with BSM. You can use the configuration file for the NetScout Event Monitor to control the data that is sent from SiteScope to BSM. For details on the file structure and syntax, see [Field Mapping Data Types](#) in the [Using SiteScope Guide](#).

## 2. Configure a NetScout Event monitor in SiteScope

You can create this monitor:

- Directly in SiteScope.
- Using the System Availability Management Administration portal in BSM.

For details on configuring the monitor settings, see ["NetScout Event Monitor Settings" below](#).

## 3. Activate NetScout EMS integration in BSM

Activate the assignment rules in BSM. For details on how to perform this task, see [NetScout nGenius Integration](#) in the [BSM Application Administration Guide](#) in the [BSM Help](#).

# UI Descriptions

## NetScout Event Monitor Settings

User interface elements are described below:

UI Element	Description
Run Alerts	<p>Method for running alerts:</p> <ul style="list-style-type: none"><li>• <b>For each event received from NetScout system.</b> The monitor triggers alerts for every matching entry found.</li></ul> <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> <ul style="list-style-type: none"><li>• <b>Once, after all events from NetScout system were received.</b> 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>

UI Element	Description
<b>EMS Time Difference</b>	<p>Value that accounts 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

User interface elements are described below:

UI 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 BSM.</p> <p>This script is not editable.</p>

## Topology Settings

User interface elements are described below:

UI Element	Description
<b>Script</b>	<p>The out-of-the-box integration script that creates a topology in BSM. The topology is based on the collected data 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 BSM's applications.</p> <p>We recommend that you use the topology settings as is (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 Editing the Topology Script in the Using SiteScope Guide.</p>

## Export to BSM Connector

User interface elements are described below:

UI Element	Description
<b>Export</b>	<p>Enables exporting technology integration monitors from SiteScope and importing them to BSM Connector as policies. This feature is supported on Technology Database Integration, Technology Log File Integration, and Technology Web Service Integration monitors with a metrics, common events, or legacy events field mapping data type only.</p> <p>Select a folder on the client file system in which to save the policy files, and click <b>Open</b> to perform the export process. For task details, see Export EMS Technology Monitors to a BSM Connector Policy in the Using SiteScope Guide.</p> <p>For details on importing policies to BSM Connector, see the BSM Connector online help system (available from the toolbar of the BSM Connector user interface).</p> <p><b>Note:</b> This button is disabled and a warning message is displayed for integration monitors where export is not supported.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Chapter 121: Technology Database Integration Monitor

The Technology Database Integration Monitor enables 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 Business Service Management as samples (one sample for each row that was returned by a SQL query).

## Note:

- If you are using SiteScope 11.30 or earlier, and SiteScope is connected to BSM 9.20 or later, you can only use previously created Technology Database Integration monitors.
- To block the creation of this monitor in the SiteScope user interface, change the `_enableEMSMonitors` property value to **false** in the `<SiteScope root directory>\groups\master.config` file, and restart SiteScope (by default, the value is set to **true**).
- For all new third-party data integrations, HPE recommends using BSM Connector. BSM Connector provides more functionality and coverage regarding the types of third-party data that can be collected than Technology Integration monitors. Note that BSM Connector works with BSM 9.20 and later only. For details on BSM Connector, see the BSM Application Administration Guide in the BSM Help.
- This monitor is not available in the user interface when using Community or Load Testing edition.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the monitor from the New Monitor Page.

## Learn About

This section includes:

- ["Technology Database Integration Monitor overview" below](#)
- ["What Data Is Forwarded" on the next page](#)
- ["Understanding How Data in the Enumerating Field is Processed" on the next page](#)
- ["Notes and Limitations" on page 863](#)

## Technology Database Integration Monitor overview

The Technology Database Integration Monitor enables you to collect data from database tables used by Enterprise Management Systems (EMS) by performing a query through a JDBC connection.

The following are examples of data that can be integrated into BSM using the Technology Database Integration Monitor:

- Events from monitoring applications event tables or views.
- Open tickets from ticketing systems applications.

- Time series data from monitoring applications metrics tables.
- Topology from a third-party topology database.

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.

## 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 data records are forwarded only once. Using an initial value enables you to specify an initial threshold value for the data that should be forwarded.

For example, if **Enumerating Field Type** uses DATE and **Start from value** uses 2003-20-03 12:00:00, only data records 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 data records are forwarded. For details on how data from the enumerating field is processed, see ["Understanding How Data in the Enumerating Field is Processed" below](#).

You use the field mapping script selected for the Technology Database Integration Monitor to control the data that is sent from SiteScope to BSM (for script types, see Field Mapping Data Types in the Using SiteScope Guide). For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide. For best practices and details on configuring the integration (depending on the type of sample data being captured), see How to Deploy Integration Monitors in the Using SiteScope Guide.

Data can also be mapped to a topology to forward data to the correct CI hierarchy in BSM. You can configure topology settings for the monitor by selecting one of the predefined scripts, or configuring your own topology script during monitor creation. For more details on editing the script, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.

Before setting up the Technology Database Integration Monitor, make sure you are clear about the purpose and usage of the data in BSM (for presentation in Service Health, Service Level Management, reports, or all).

## Understanding How Data in the Enumerating Field is Processed

Since the data in the enumerating field is not unique key, the data in the column used for the enumerating field must have constantly increasing values or values that changed since the scheduled monitor run. For example, if before the first monitor run the table contains the following data:

**Run 1:**

ENUM_FIELD	DATA_NAME
1	Alice
1	Alice
2	Bob

The monitor reads all entries, stores "1" as the position where all data was send, and skips the lines with ENUM\_FIELD=2, because there is a possibility that new lines with ENUM\_FIELD=2 will be added later.

**Run 2:**

ENUM_FIELD	DATA_NAME
1	Alice
1	Alice
2	Bob
2	Bob
2	Bob

At the end of the run, the monitor runs a query with filter "where ENUM\_FIELD>1". However, it does not send any data because it did not reach the end of the values listed as having ENUM\_FIELD=2. The monitor cannot send this partial list until a new higher value appears in the table.

### Run 3:

ENUM_FIELD	DATA_NAME
1	Alice
1	Alice
2	Bob
2	Bob
2	Bob
3	Charlie

At this stage, the monitor runs the same query with filter "where ENUM\_FIELD>1", and sends all the data with ENUM\_FIELD equals to 2. It also updates the internal variable for last read position to 2, and skips the last line with ENUM\_FIELD equals to 3, until new lines with a value higher than 3 appears.

## 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.

## Tasks

### How to Integrate database data into BSM

This section provides the workflow for setting up the Technology Database Integration Monitor to work with BSM.

#### 1. Prerequisites

- Integration monitors are available for creation in specific instances only. For details, see the note at the top of this chapter.
- Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see *How to Configure SiteScope to Communicate with BSM* in the *Using SiteScope Guide*.
- There are several key database driver requirements for using this monitor.
  - You can use the database drivers supplied with SiteScope by default, or you can 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. If the file is in zip format, unzip the contents to a temporary directory. 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:
    - **com.mercury.jdbc.sqlserver.SQLServerDriver**. DataDirect driver from DataDirect Technologies. It is a driver for those Microsoft SQL databases that use Windows authentication. For details on installing the driver, see the note below.

**Note:** To install the MSSQL JDBC driver:

- Download the MSSQL JDBC driver from the [Microsoft Download Center](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2505) (<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2505>), and unzip the contents to a temporary directory.
- Copy the **sqljdbc4.jar** file to the **<SiteScope root directory>\WEB-INF\lib** subdirectory.
- Restart the **SiteScope** service.
- Use the Database Connection Tool for connection tuning:
  - Database Connection URL:** `jdbc:sqlserver://<IP Address>:<port>;InstanceName=<name>;DatabaseName=<name>`
  - Database Driver:** `com.microsoft.sqlserver.jdbc.SQLServerDriver`
- Create the desired database monitor type.

- **com.mercury.jdbc.oracle.OracleDriver**. A driver for Oracle databases. When using the driver deployed with SiteScope, the database connection URL has the form of:  
`jdbc:mercury:oracle://<server name or IP address>:<database server`



port>;sid=<sid>

**Note:** The URL format may differ if you are using another JDBC driver, since the JDBC URL depends on the driver.

- **oracle.jdbc.driver.OracleDriver.** SiteScope supports the following categories of JDBC driver supplied by Oracle that are compatible with Java 7:
  - JDBC thin driver for Oracle databases.
  - JDBC OCI (thick) driver. For details on accessing Oracle databases using OCI driver, see ["How to access Oracle databases using OCI driver" on page 165.](#)
- **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. Database Connection URLs for this monitor are:
  - **jdbc:mercury:sqlserver://<hostname>:1433;DatabaseName=master;AuthenticationMethod=type2**  
where <hostname> is the name of the host where the database is running.
  - **jdbc:mercury:oracle://<hostname or IP address>:<port>;sid=<sid>**  
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 <sid> is the Oracle system ID.
  - **jdbc:oracle:thin:@<hostname/FQDN>:<port>/<service>**  
where <hostname/FQDN> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <service> is the Oracle service name.
- 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.
- Use a database client to connect to the relevant software database. Identify which tables contain the required data (the software schema documentation may help you with this).

## 2. Use the SiteScope Database Connection tool

Run the SiteScope Database Connection tool (for details, see Database Connection Tool in the Using SiteScope Guide) 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 BSM.

## 3. Create a Technology Database Integration monitor

Add a Technology Database Integration Monitor to SiteScope. For monitor user interface details, see ["Technology Database Integration Monitor Settings" on the next page](#).

- 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 mapping

The mapping defines the processing of incoming data and the output sample forwarded to BSM.

**Note:** The Field Mapping panel is not available when the **Report topology without data** check box is selected in Topology Settings.

- a. In the New Technology Database Integration Monitor dialog box, expand the **Field Mapping** panel. Select a field mapping type and click **Load File**. For details on field mapping types, see Field Mapping Data Types in the Using SiteScope Guide.  
For user interface details, see ["Field Mapping" on page 870](#).
- b. 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 BSM. For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide.

#### 5. Edit the monitor's topology settings - optional

In the **Topology Settings** panel, you can create or select a script that creates a topology of configuration items in BSM's RTSM to match your EMS system.

For details on this topic, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.

For user interface details, see ["Topology Settings" on page 871](#).

#### 6. View data from the monitor in BSM

View the data in BSM:

- If you chose and edited the **Common Events/Legacy Events** script in the Field Mapping panel, you can view events in Service Health, System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.

- If you chose and edited the **Metrics** script in the Field Mapping panel, 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 **<BSM root directory>\bin**.
- To troubleshoot problems with data arriving to BSM, see ["Troubleshooting" on page 873](#).

## UI Descriptions

### Technology Database Integration Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Basic Settings</b>	
<b>Database connection URL</b>	URL to a database connection (sometimes referred to as an Authentication string).  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.
<b>Database driver</b>	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>	User name used to log on to the database.
<b>Database password</b>	Password used to log on to the database.
<b>OS integrated security</b>	Uses the user name and password from Windows' user authentication to access the database. Entries in the Database Username and Database Password are ignored.  If this parameter is checked, you must use the DataDirect driver as your database driver.
<b>EMS server name</b>	Text identifier describing the database server that this monitor is monitoring if you are reporting monitor data to an installation of Business Service Management. This text descriptor is used to identify the database server when the monitor data is viewed in an Business Service Management report.  <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 machine.

UI Element	Description
<b>EMS time difference</b>	<p>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>Timeout</b>	<p>Amount of time, in seconds, that SiteScope should wait before the monitor times out.</p> <p><b>Default value:</b> 60 seconds</p>
<b>Query Settings</b>	
<b>SELECT</b>	<p>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>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>
<b>WHERE</b>	<p>WHERE clause to be used in the SQL query. This is an optional field which enables 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>Name for a database field that can be used to order the data that is returned from the database query.</p> <p>For details on how data from the enumerating field is processed, see <a href="#">"Understanding How Data in the Enumerating Field is Processed"</a> on page 862.</p> <p><b>Note:</b> The column used as enumerating field must be included in the SELECT clause.</p>

UI Element	Description																			
<b>Enumerating field type</b>	<p>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> <tr> <th>SQL Type</th><th>Enumerating Field Type</th></tr> <tr> <td>SMALLINT</td><td>INTEGER</td></tr> <tr> <td>INTEGER</td><td>INTEGER / LONG</td></tr> <tr> <td>BIGINT</td><td>LONG</td></tr> <tr> <td>NUMERIC</td><td>LONG</td></tr> <tr> <td>DOUBLE</td><td>DOUBLE</td></tr> <tr> <td>DECIMAL</td><td>DOUBLE</td></tr> <tr> <td>FLOAT</td><td>DOUBLE</td></tr> <tr> <td>TIMESTAMP</td><td>TIMESTAMP</td></tr> <tr> <td>DATE</td><td>TIMESTAMP</td></tr> </table>	SQL Type	Enumerating Field Type	SMALLINT	INTEGER	INTEGER	INTEGER / LONG	BIGINT	LONG	NUMERIC	LONG	DOUBLE	DOUBLE	DECIMAL	DOUBLE	FLOAT	DOUBLE	TIMESTAMP	TIMESTAMP	DATE
SQL Type	Enumerating Field Type																			
SMALLINT	INTEGER																			
INTEGER	INTEGER / LONG																			
BIGINT	LONG																			
NUMERIC	LONG																			
DOUBLE	DOUBLE																			
DECIMAL	DOUBLE																			
FLOAT	DOUBLE																			
TIMESTAMP	TIMESTAMP																			
DATE	TIMESTAMP																			
<b>Initial enumerating value</b>	<p>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>Initial enumerating value</b> 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>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 java.lang.OutOfMemoryException 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

User interface elements are described below:

UI Element	Description
<b>Data Type</b>	<p>Select from the following data types for this integration:</p> <ul style="list-style-type: none"> <li>• <b>Common Events.</b> For details, see Configuring Field Mapping for Common Event Samples in the Using SiteScope Guide.</li> <li>• <b>Legacy Events.</b> For details, see Configuring Field Mapping for Legacy Event Samples in the Using SiteScope Guide.</li> <li>• <b>Metrics.</b> For details, see Configuring Field Mapping for Metrics Samples in the Using SiteScope Guide.</li> <li>• <b>Tickets.</b> For details, see Configuring Field Mapping for Ticket Samples in the Using SiteScope Guide.</li> </ul>
<b>Load File</b>	<p>Loads the script that is applicable to the data 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 BSM. To enable the integration, you must configure the mapping as required by the environment you are monitoring.</p> <p>The mapping is editable in this box using the script editor provided (you can make the script field read only by right-clicking the script and selecting <b>Configure &gt; Read Only</b>). 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 Field Mapping Data Types in the Using SiteScope Guide.</p>
<b>Test Script</b>	<p>Tests 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 metrics are forwarded to BSM.</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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Topology Settings

User interface elements are described below:

UI Element	Description
<b>Report topology without data</b>	<p>Reports the topology for the integration monitor without sending the data samples to BSM. When this option is selected, the Field Mapping panel is not available.</p> <p><b>Default value:</b> Not selected</p>
<b>Topology script</b>	<p>Script to create the topology in BSM for the samples retrieved from the monitored third-party application. The script is based on the Jython scripting language (Python enabled by Java). The monitor propagates its status to the CIs mapped in this topology. The template options displayed depend on the data type selected in the Field Mapping panel.</p> <p><b>For Event data type:</b></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 Computer or Running Software CIs.</li> <li>• <b>Computer.</b> Creates a topology with a Computer CI. Available for Common Event samples only.</li> <li>• <b>Computer - Running Software.</b> Creates a topology with a Computer CI and a Running Software CI connected to it with a <i>Composition</i> relationship. Available for Common Event samples only.</li> </ul> <p><b>Note:</b> Legacy Event samples (<b>Node</b> and <b>Node - Running Software</b>) are also available. For details, see Legacy Topology Scripts in the Using SiteScope Guide.</p> <p><b>For Metrics data type:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer - Monitor.</b> Sends the SiteScope topology with SiteScope Monitor and Computer CIs. If selected, the script area is not available.</li> </ul> <p>The <b>Computer - Monitor</b> topology integration requires that the names or IP addresses of the nodes that it adds to RTSM are accessible through DNS resolution. To successfully populate a Node CI specified in the <i>TargetName</i> field to RTSM, SiteScope must be able to resolve the node's fully qualified domain name and IP address through a DNS service.</p> <ul style="list-style-type: none"> <li>• <b>No Topology.</b> No topology is sent (although data is still sent). If selected, the script area is not available.</li> </ul> <p><b>For Tickets data type:</b></p> <ul style="list-style-type: none"> <li>• <b>Tickets.</b> Creates a Business Service CI with an EMS monitor CI connected to it with <i>Monitored By</i> relationship.</li> </ul> <p><b>Note:</b> Only select <b>Custom</b> if you are familiar with the Jython language, because you must create the topology script in Jython yourself. Depending on the data type you select, we recommend that you begin with and edit one of the predefined scripts.</p> <p>For more details, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.</p>

UI Element	Description
<b>Load Script</b>	Loads the required 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. The script is based on the Jython scripting language (Python enabled by Java).
<b>Script</b>	<p>The contents of the script are visible in this box. You can edit the script contents in this field using the script editor provided by SiteScope, or you can copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p><b>Note:</b> The topology script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see Editing the Topology Script in the Using SiteScope Guide.</p>
<b>Test Script</b>	<p>Tests the topology script. We recommend that you test the script before running the monitor. This test gives you the results of what events or metrics are forwarded to BSM 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: <b>&lt;SiteScope root directory&gt;\logs\bac_integration.log</b>.</p> <p><b>Note:</b> The test does not forward samples to BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Export to BSM Connector

User interface elements are described below:

UI Element	Description
<b>Export</b>	<p>Enables exporting technology integration monitors from SiteScope and importing them to BSM Connector as policies. This feature is supported on Technology Database Integration, Technology Log File Integration, and Technology Web Service Integration monitors with a metrics, common events, or legacy events field mapping data type only.</p> <p>Select a folder on the client file system in which to save the policy files, and click <b>Open</b> to perform the export process. For task details, see Export EMS Technology Monitors to a BSM Connector Policy in the Using SiteScope Guide.</p> <p>For details on importing policies to BSM Connector, see the BSM Connector online help system (available from the toolbar of the BSM Connector user interface).</p> <p><b>Note:</b> This button is disabled and a warning message is displayed for integration monitors where export is not supported.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.



# Troubleshooting

## Debugging Errors/Troubleshooting

This section describes troubleshooting and limitations when working with the Technology Database Integration monitor.

- 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 **Service Health/Event Log/SiteScope reports**, look in **<BSM 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 Service Health to verify that Service Health received the samples. Open the following file on the Gateway Server machine:  
**<BSM 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.IgnoredSamples  
Logger=${logLevel}, IgnoredSamples.appender`
  - `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisher  
Samples=${logLevel}, PublishedSamples.appender`

Look at the corresponding log files:

- **<BSM root directory>\logs\mercury\_wde\wdeIgnoredSamples.log**
- **<BSM root directory>\logs\mercury\_wde\wdePublishedSamples.log**

# Chapter 122: 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 BSM.

## Note:

- If you are using SiteScope 11.30 or earlier, and SiteScope is connected to BSM 9.20 or later, you can only use previously created Technology Log File Integration monitors.
- To block the creation of this monitor in the SiteScope user interface, change the `_enableEMSMonitors` property value to **false** in the `<SiteScope root directory>\groups\master.config` file, and restart SiteScope (by default, the value is set to **true**).
- For all new third-party data integrations, HPE recommends using BSM Connector. BSM Connector provides more functionality and coverage regarding the types of third-party data that can be collected than Technology Integration monitors. Note that BSM Connector works with BSM 9.20 and later only. For details on BSM Connector, see the BSM Application Administration Guide in the BSM Help.
- This monitor is not available in the user interface when using Community or Load Testing edition.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the monitor from the New Monitor Page.

## Learn About

This section includes:

- ["Technology Log File Integration Monitor Overview" below](#)
- ["What Data Is Collected" on the next page](#)

## Technology Log File Integration Monitor Overview

Each time that SiteScope runs the Technology Log File Integration monitor, the monitor starts from the point in the log 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 BSM. For details on using back references, see Retaining Content Match Values in the Using SiteScope Guide.

**Note:** 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 BSM. For examples of regular expressions, see Examples for Log File Monitoring in the Using SiteScope Guide.

## What Data Is Collected

The Technology Log File Integration monitor sends to BSM data that is extracted from any row that matched against the **Content match** regular expression.

Before setting up the Technology Log File Integration Monitor, make sure you are clear about the purpose and usage of the data in BSM (for presentation in Service Health, Service Level Management, and reports).

The specific data that is forwarded to BSM is controlled by the field mapping script (for script types, see Field Mapping Data Types in the Using SiteScope Guide). You use this script to specify the preferred value fields that you want forwarded. For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide. For best practices and details on configuring the integration (depending on the type of sample data being captured), see How to Deploy Integration Monitors in the Using SiteScope Guide.

Data can also be mapped to a topology to forward data to the correct CI hierarchy in BSM. You can configure topology settings for the monitor by selecting one of the predefined scripts, or configuring your own topology script during monitor creation. For more details on editing the script, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.

## Tasks

### How to integrate data from a Technology Log File

This section provides the overall flow for setting up the Technology Log File Integration Monitor to work with BSM. If you need more information on performing any of the steps, see ["Technology Log File Integration Monitor Settings" on page 877](#).

#### 1. Prerequisites

- Integration monitors are available for creation in specific instances only. For details, see the note at the top of this chapter ["Integration Monitors \(A-Z\)" on page 840](#)
- Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see How to Configure the Integration Between SiteScope and BSM in the Using SiteScope Guide.

#### 2. Analyze the log file to be monitored

Open the relevant software log file, and identify which lines describe events or metrics. 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 user interface details, see Regular Expression Tool in the Using SiteScope Guide.

#### 3. Create a Technology Log File Integration monitor

Add a Technology Log File Integration Monitor to SiteScope. For user interface details, see ["Technology Log File Integration Monitor Settings" on page 877](#).

- 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.

#### 4. Edit the monitor's field mapping

The mapping defines the processing of incoming data and the output sample forwarded to BSM.

**Note:** The Field Mapping panel is not available when the **Report topology without data** check box is selected in Topology Settings.

- a. In the New Technology Log File Integration Monitor dialog box, expand the **Field Mapping** panel. Select a field mapping type and click **Load File**. For details on field mapping types, see Field Mapping Data Types in the Using SiteScope Guide.  
For user interface details, see ["Field Mapping" on page 880](#).
- b. 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 BSM. For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide.

**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)
```

#### 5. Edit the monitor's topology settings - optional

In the **Topology Settings** panel, you can create or select a script that creates a topology of configuration items in BSM's RTSM to match your EMS system.

For details on this topic, see [Topology Settings for Technology Integration Monitors](#) in the Using SiteScope Guide.

For user interface details, see ["Topology Settings" on page 881](#).

## 6. 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 user interface details, see [Regular Expression Tool](#) in the Using SiteScope Guide.

## 7. View data from the monitor in BSM

View the data in BSM:

- If you chose and edited the **Common Events/Legacy Events** script in the Field Mapping panel, you can view events in Service Health, System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- If you chose and edited the **Tickets** script in the Field Mapping panel, you can view events in any application that supports SiteScope data, including SiteScope Over Time reports.
- If you chose and edited the **Metrics** script in the Field Mapping panel, 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 **<BSM root directory>\bin**.
- To troubleshoot problems with data arriving to BSM, see ["Troubleshooting" on page 883](#).

# UI Descriptions

## Technology Log File Integration Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Monitor Settings</b>	
<b>Server</b>	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.  <b>Default value:</b> SiteScope Server (the server on which SiteScope is installed)

UI Element	Description
<b>Log file path name</b>	<p>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 log on to the remote machine. Select <b>Remote Servers &gt; UNIX Remote Servers</b> for information about which UNIX user account is being used.</li> <li>• <b>Remote Windows 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 Windows connection profiles (displayed in the Microsoft Windows remote server list). If an exact match is found for <code>\\remoteserver</code> in the remote Windows 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. It is not necessary to select a remote Windows server if you are using NetBIOS to connect to remote Windows servers.</li> <li>• <b>Remote Windows through SSH.</b> Select a remote server from the drop-down list. The path of the log file depends on the type of SSH server installed on the remote Windows server: <ul style="list-style-type: none"> <li>• SSH servers that provide a UNIX-like interface (for example, Cygwin OpenSSH): <code>/cygdrive/&lt;drive_letter&gt;/&lt;directory&gt;/filename.log</code></li> <li>• SSH servers that provide a Windows command prompt (for example, OpenSSH for Windows): <code>&lt;drive_letter&gt;:\&lt;folder&gt;\filename.log</code></li> </ul> </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>
<b>Content match</b>	<p>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 <b>s</b> search modifier to the end of the regular expression. For details on regular expressions, see Regular Expressions Overview in the Using SiteScope Guide.</p>

UI Element	Description
<b>Open Tool</b>	Opens the Regular Expression Tool, enabling 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 in the Using SiteScope Guide.
<b>No error if file not found</b>	Keeps the monitor in good status if the file is not found.
<b>Log file encoding</b>	Log file encoding that is used if you are reading a log file whose encoding is different than the SiteScope machine's default encoding.  <b>Default value:</b> windows-1252
<b>Run alerts</b>	<p>Method for running alerts for this monitor:</p> <ul style="list-style-type: none"> <li>• <b>For each log entry matched.</b> Triggers alerts for each matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error). <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 <code>Error if</code> or <code>Warning if</code> thresholds are defined accordingly (for example, setting <code>Error if</code> to the default of <code>matchCount &gt; 0</code>).</li> <li>• <b>Once, after all log entries have been checked.</b> Counts 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. <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 <code>&lt;matchDetails&gt;</code> 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.  Email alert templates are stored in the <code>&lt;SiteScope root directory&gt;\templates.mail</code> directory.</li> </ul>
<b>EMS time difference</b>	<p>Value that accounts 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>Timeout Settings</b>	

UI Element	Description
<b>Enable timeout</b>	The monitor stops its run after the specified timeout period has been exceeded. <b>Default value:</b> Not selected
<b>After timeout, resume reading from end of file</b>	If selected, the monitor resumes reading from the end of the log file during the next run, instead of from the current location. <b>Default value:</b> Selected <b>Note:</b> This setting is only available when <b>Enable timeout</b> is selected.
<b>Status after timeout</b>	The status condition that the monitor goes into if the monitor times out. The status categories include: Error, Warning, Good <b>Default value:</b> Warning <b>Note:</b> This setting is only available when <b>Enable timeout</b> is selected.
<b>Timeout (seconds)</b>	Amount of time, in seconds, that SiteScope should wait before the monitor times out. <b>Default value:</b> 60 seconds <b>Note:</b> This setting is only available when <b>Enable timeout</b> is selected.

## Field Mapping

User interface elements are described below:

UI Element	Description
<b>Data Type</b>	Select from the following data types for this integration: <ul style="list-style-type: none"> <li>• <b>Common Events.</b> For details, see Configuring Field Mapping for Common Event Samples in the Using SiteScope Guide.</li> <li>• <b>Legacy Events.</b> For details, see Configuring Field Mapping for Legacy Event Samples in the Using SiteScope Guide.</li> <li>• <b>Metrics.</b> For details, see Configuring Field Mapping for Metrics Samples in the Using SiteScope Guide.</li> <li>• <b>Tickets.</b> For details, see Configuring Field Mapping for Ticket Samples in the Using SiteScope Guide.</li> </ul>
<b>Load File</b>	Loads the script that is applicable to the data type selected above.



UI 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 BSM. To enable the integration, you must configure the mapping as required by the environment you are monitoring.</p> <p>The mapping is editable in this box using the script editor provided (you can make the script field read only by right-clicking the script and selecting <b>Configure &gt; Read Only</b>). 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 Field Mapping Data Types in the Using SiteScope Guide.</p>
<b>Test Script</b>	<p>Tests 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 metrics are forwarded to BSM. 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Topology Settings

User interface elements are described below:

UI Element	Description
<b>Report topology without data</b>	<p>Reports the topology for the integration monitor without sending the data samples to BSM. When this option is selected, the Field Mapping panel is not available.</p> <p><b>Default value:</b> Not selected</p>

UI Element	Description
<b>Topology script</b>	<p>Script to create the topology in BSM for the samples retrieved from the monitored third-party application. The script is based on the Jython scripting language (Python enabled by Java). The monitor propagates its status to the CIs mapped in this topology. The template options displayed depend on the data type selected in the Field Mapping panel.</p> <p><b>For Event data type:</b></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 Computer or Running Software CIs.</li> <li>• <b>Computer.</b> Creates a topology with a Computer CI. Available for Common Event samples only.</li> <li>• <b>Computer - Running Software.</b> Creates a topology with a Computer CI and a Running Software CI connected to it with a <i>Composition</i> relationship. Available for Common Event samples only.</li> </ul> <p><b>Note:</b> Legacy Event samples (<b>Node</b> and <b>Node - Running Software</b>) are also available. For details, see Legacy Topology Scripts in the Using SiteScope Guide.</p> <p><b>For Metrics data type:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer - Monitor.</b> Sends the SiteScope topology with Sitescope Monitor and Computer CIs. If selected, the script area is not available.</li> </ul> <p>The <b>Computer - Monitor</b> topology integration requires that the names or IP addresses of the nodes that it adds to RTSM are accessible through DNS resolution. To successfully populate a Node CI specified in the <i>TargetName</i> field to RTSM, SiteScope must be able to resolve the node's fully qualified domain name and IP address through a DNS service.</p> <ul style="list-style-type: none"> <li>• <b>No Topology.</b> No topology is sent (although data is still sent). If selected, the script area is not available.</li> </ul> <p><b>For Tickets data type:</b></p> <ul style="list-style-type: none"> <li>• <b>Tickets.</b> Creates a Business Service CI with an EMS monitor CI connected to it with <i>Monitored By</i> relationship.</li> </ul> <p><b>Note:</b> Only select <b>Custom</b> if you are familiar with the Jython language, because you must create the topology script in Jython yourself. Depending on the data type you select, we recommend that you begin with and edit one of the predefined scripts.</p> <p>For more details, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.</p>
<b>Load Script</b>	<p>Loads the required 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. The script is based on the Jython scripting language (Python enabled by Java).</p>

UI Element	Description
<b>Script</b>	<p>The contents of the script are visible in this box. You can edit the script contents in this field using the script editor provided by SiteScope, or you can copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p><b>Note:</b> The topology script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see Editing the Topology Script in the Using SiteScope Guide.</p>
<b>Test Script</b>	<p>Tests 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 metrics are forwarded to BSM 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: <b>&lt;SiteScope root directory&gt;\logs\bac_integration.log</b>.</p> <p><b>Note:</b> The test does not forward samples to BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Export to BSM Connector

User interface elements are described below:

UI Element	Description
<b>Export</b>	<p>Enables exporting technology integration monitors from SiteScope and importing them to BSM Connector as policies. This feature is supported on Technology Database Integration, Technology Log File Integration, and Technology Web Service Integration monitors with a metrics, common events, or legacy events field mapping data type only.</p> <p>Select a folder on the client file system in which to save the policy files, and click <b>Open</b> to perform the export process. For task details, see Export EMS Technology Monitors to a BSM Connector Policy in the Using SiteScope Guide.</p> <p>For details on importing policies to BSM Connector, see the BSM Connector online help system (available from the toolbar of the BSM Connector user interface).</p> <p><b>Note:</b> This button is disabled and a warning message is displayed for integration monitors where export is not supported.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Troubleshooting

## Debugging Errors/Troubleshooting

This section describes troubleshooting and limitations when working with the Technology Log File Integration

monitor.

- 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 **Service Health/Event Log/SiteScope reports**, look in **<BSM 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 Service Health to verify that Service Health received the samples. Open the following file on the Gateway Server machine:  
**<BSM 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.IgnoredSamples  
Logger=${loglevel}, IgnoredSamples.appender`
- `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisher  
Samples=${loglevel}, PublishedSamples.appender`

Look at the corresponding log files:

- **<BSM root directory>\logs\mercury\_wde\wdeIgnoredSamples.log**
- **<BSM root directory>\logs\mercury\_wde\wdePublishedSamples.log**

# Chapter 123: 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 BSM containing the SNMP trap values. The third-party EMS systems must be configured to send traps to the SiteScope server.

## Note:

- If you are using SiteScope 11.30 or earlier, and SiteScope is connected to BSM 9.20 or later, you can only use previously created Technology SNMP Trap Integration monitors.
- To block the creation of this monitor in the SiteScope user interface, change the `_enableEMSMonitors` property value to **false** in the `<SiteScope root directory>\groups\master.config` file, and restart SiteScope (by default, the value is set to **true**).
- For all new third-party data integrations, HPE recommends using BSM Connector. BSM Connector provides more functionality and coverage regarding the types of third-party data that can be collected than Technology Integration monitors. Note that BSM Connector works with BSM 9.20 and later only. For details on BSM Connector, see the BSM Application Administration Guide in the BSM Help.
- This monitor is not available in the user interface when using Community or Load Testing edition.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the monitor from the New Monitor Page.

## Learn About

This section includes:

- ["Technology SNMP Trap Integration Monitor Overview" below](#)
- ["What Data Is Collected" below](#)
- ["IPv6 Addressing Supported Protocols" on the next page](#)

## Technology SNMP Trap Integration Monitor Overview

The Technology SNMP Trap Integration Monitor is useful for integrating traps that your external devices create into the BSM framework. For example, you can use this monitor to forward information from Network Node Manager to BSM. For more information, see Network Node Manager Integration Overview in the Using SiteScope Guide.

## 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 BSM containing preferred values from the original SNMP trap.

Before setting up the Technology SNMP Trap Integration Monitor, make sure you are clear about the purpose and usage of the data in BSM (for presentation in Service Health, Service Level Management, reports, or all).

The specific data that is forwarded to BSM is controlled by the field mapping script (for script types, see Field Mapping Data Types in the Using SiteScope Guide). You use this script to specify the preferred value fields that you want forwarded. For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide. For best practices and details on configuring the integration (depending on the type of sample data being captured), see How to Deploy Integration Monitors in the Using SiteScope Guide.

Data can also be mapped to a topology to forward data to the correct CI hierarchy in BSM. You can configure topology settings for the monitor by selecting one of the predefined scripts, or configuring your own topology script during monitor creation. For more details on editing the script, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.

## IPv6 Addressing Supported Protocols

When **Prefer IP version 6 addresses** is enabled in SiteScope (**Preferences > Infrastructure Preferences > Server Settings**), this monitor supports the SNMP protocol.

For details on using IPv6, see Support for IP Version 6 in the Using SiteScope Guide.

# Tasks

## How to integrate data from an SNMP trap

This section provides the overall flow for setting up the Technology SNMP Trap Integration Monitor to work with BSM. If you need more information on performing any of the steps, see the section on ["Technology SNMP Trap Monitor Settings " on page 889](#).

### 1. Prerequisites

- Integration monitors are available for creation in specific instances only. For details, see the note at the top of this chapter ["Integration Monitors \(A-Z\)" on page 840](#)
- Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see How to Configure the Integration Between SiteScope and BSM in the Using SiteScope Guide.

### 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 <http://live.sysinternals.com/>.

d. Restart SiteScope.

#### 4. Create a Technology SNMP Trap Integration monitor

Add a Technology SNMP Trap Integration Monitor to SiteScope. For monitor user interface details, see "[Technology SNMP Trap Monitor Settings](#)" on page 889.

**Note:**

- 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.
- The **SNMP Trap Tool** 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 **Use monitor tools** permissions). To use the tool when configuring or editing a monitor, click the **Use Tool** button. For details on the tool, see SNMP Trap Tool in the Using SiteScope Guide.

#### 5. Edit the monitor's field mapping

The mapping defines the processing of incoming data and the output sample forwarded to BSM.

**Note:** The Field Mapping panel is not available when the **Report topology without data** check box is selected in Topology Settings.

- a. In the New Technology SNMP Trap Integration Monitor dialog box, expand the **Field Mapping** panel. Select a field mapping type and click **Load File**. For details on field mapping types, see Field Mapping Data Types in the Using SiteScope Guide.

For user interface details, see "[Field Mapping](#)" on page 889.

- b. 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 BSM. For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide.

**Note:**

- When using this monitor with v2 traps, `traptime` and `oid` are undefined. Use the following structure instead:  
`var1` instead of `traptime`  
`var2` instead of `oid`  
`var3` instead of `var1`  
.....  
`var{N+2}` instead of `var{N}`
- 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.

## 6. Edit the monitor's topology settings - optional

In the **Topology Settings** panel, you can create or select a script that creates a topology of configuration items in BSM's RTSM to match your EMS system.

For details on this topic, see *Topology Settings for Technology Integration Monitors* in the *Using SiteScope Guide*.

For user interface details, see ["Topology Settings" on page 890](#).

## 7. View data from the monitor in BSM

View the data in BSM:

- 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.snmpwalk.org](http://www.snmpwalk.org).)
- If you chose and edited the **Common Events/Legacy Events** script in the Field Mapping panel, you can view events in Service Health, System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- If you chose and edited the **Metrics** script in the Field Mapping panel, 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 **<BSM root directory>\bin**.
- To troubleshoot problems with data arriving to BSM, see ["Troubleshooting" on page 892](#).



## UI Descriptions

### Technology SNMP Trap Monitor Settings

User interface elements are described below:

UI Element	Description
<b>Run alerts</b>	<p>Method for running alerts:</p> <ul style="list-style-type: none"><li>• <b>For each SNMP Trap received from EMS system.</b> The monitor triggers alerts for every matching entry found.</li></ul> <p>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.</p> <ul style="list-style-type: none"><li>• <b>Once, after all SNMP Traps from EMS system were received.</b> 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>
<b>EMS time difference</b>	<p>Value that accounts 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

User interface elements are described below:

UI Element	Description
<b>Data Type</b>	<p>Select from the following data types for this integration:</p> <ul style="list-style-type: none"><li>• <b>Common Events.</b> For details, see Configuring Field Mapping for Common Event Samples in the Using SiteScope Guide.</li><li>• <b>Legacy Events.</b> For details, see Configuring Field Mapping for Legacy Event Samples in the Using SiteScope Guide.</li><li>• <b>Metrics.</b> For details, see Configuring Field Mapping for Metrics Samples in the Using SiteScope Guide.</li><li>• <b>Tickets.</b> For details, see Configuring Field Mapping for Ticket Samples in the Using SiteScope Guide.</li></ul>

UI Element	Description
<b>Load File</b>	Loads the script that is applicable to the data 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 BSM. To enable the integration, you must configure the mapping as required by the environment you are monitoring.</p> <p>The mapping is editable in this box using the script editor provided (you can make the script field read only by right-clicking the script and selecting <b>Configure &gt; Read Only</b>). 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 Field Mapping Data Types in the Using SiteScope Guide.</p>
<b>Test Script</b>	<p>Tests 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 metrics are forwarded to BSM. 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Topology Settings

User interface elements are described below:

UI Element	Description
<b>Report topology without data</b>	<p>Reports the topology for the integration monitor without sending the data samples to BSM. When this option is selected, the Field Mapping panel is not available.</p> <p><b>Default value:</b> Not selected</p>

UI Element	Description
<b>Topology script</b>	<p>Script to create the topology in BSM for the samples retrieved from the monitored third-party application. The script is based on the Jython scripting language (Python enabled by Java). The monitor propagates its status to the CIs mapped in this topology. The template options displayed depend on the data type selected in the Field Mapping panel.</p> <p><b>For Event data type:</b></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 Computer or Running Software CIs.</li> <li>• <b>Computer.</b> Creates a topology with a Computer CI. Available for Common Event samples only.</li> <li>• <b>Computer - Running Software.</b> Creates a topology with a Computer CI and a Running Software CI connected to it with a <i>Composition</i> relationship. Available for Common Event samples only.</li> </ul> <p><b>Note:</b> Legacy Event samples (<b>Node</b> and <b>Node - Running Software</b>) are also available. For details, see Legacy Topology Scripts in the Using SiteScope Guide.</p> <p><b>For Metrics data type:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer - Monitor.</b> Sends the SiteScope topology with Sitescope Monitor and Computer CIs. If selected, the script area is not available.</li> </ul> <p>The <b>Computer - Monitor</b> topology integration requires that the names or IP addresses of the nodes that it adds to RTSM are accessible through DNS resolution. To successfully populate a Node CI specified in the <i>TargetName</i> field to RTSM, SiteScope must be able to resolve the node's fully qualified domain name and IP address through a DNS service.</p> <ul style="list-style-type: none"> <li>• <b>No Topology.</b> No topology is sent (although data is still sent). If selected, the script area is not available.</li> </ul> <p><b>For Tickets data type:</b></p> <ul style="list-style-type: none"> <li>• <b>Tickets.</b> Creates a Business Service CI with an EMS monitor CI connected to it with <i>Monitored By</i> relationship.</li> </ul> <p><b>Note:</b> Only select <b>Custom</b> if you are familiar with the Jython language, because you must create the topology script in Jython yourself. Depending on the data type you select, we recommend that you begin with and edit one of the predefined scripts.</p> <p>For more details, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.</p>
<b>Load Script</b>	<p>Loads 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. The script is based on the Jython scripting language (Python enabled by Java).</p>

UI Element	Description
<b>Script</b>	<p>The contents of the script are visible in this box. You can edit the script contents in this field using the script editor provided by SiteScope, or you can also copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p><b>Note:</b> The topology script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see Editing the Topology Script in the Using SiteScope Guide.</p>
<b>Test Script</b>	<p>Tests the topology script. We recommend that you test the script before running the monitor. This test gives you the results of what events or metrics are forwarded to BSM 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: <b>&lt;SiteScope root directory&gt;\logs\bac_integration.log</b>.</p> <p><b>Note:</b> The test does not forward samples to BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Export to BSM Connector

User interface elements are described below:

UI Element	Description
<b>Export</b>	<p>Enables exporting technology integration monitors from SiteScope and importing them to BSM Connector as policies. This feature is supported on Technology Database Integration, Technology Log File Integration, and Technology Web Service Integration monitors with a metrics, common events, or legacy events field mapping data type only.</p> <p>Select a folder on the client file system in which to save the policy files, and click <b>Open</b> to perform the export process. For task details, see Export EMS Technology Monitors to a BSM Connector Policy in the Using SiteScope Guide.</p> <p>For details on importing policies to BSM Connector, see the BSM Connector online help system (available from the toolbar of the BSM Connector user interface).</p> <p><b>Note:</b> This button is disabled and a warning message is displayed for integration monitors where export is not supported.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

## Troubleshooting

This section contains:

- ["Basic Troubleshooting Guidelines" below](#)
- ["Verify SNMP Trap Reception to SiteScope" below](#)
- ["Common Problems and Solutions" below](#)

## 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 Service Health to verify that Service Health received the samples. Open the following file on the Gateway Server machine:  
**<BSM 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.IgnoredSamples  
Logger=${loglevel}, IgnoredSamples.appender`
- `log4j.category.com.mercury.am.platform.wde.publish_SamplePublisher  
Samples=${loglevel}, PublishedSamples.appender`

Refer to the following log files:

- **<BSM root directory>\logs\mercury\_wde\wdeIgnoredSamples.log**
- **<BSM 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.

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.
The SNMP traps are not forwarded to BSM applications.	The SNMP Agent does not emit SNMP traps.	Verify that the SNMP Agent is configured to emit SNMP traps. Use the <b>&lt;SiteScope&gt;\logs\snmptrap.log</b> file to verify that traps are received by SiteScope.
	The EMS configuration file contains errors.	Click the <b>Test Script</b> button in the Field Mapping panel to verify the field mapping.
	The SNMP trap port is busy.	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 operating system.
	The monitor is not configured to report to these applications.	Make sure that the monitor is configured to report to these applications.
Samples are created and sent from SiteScope, but the data is not seen in Service Health/Event Log/SiteScope reports.	Samples were dropped due to missing fields or values.	Check in <b>&lt;BSM root directory&gt;\log\mercury_wde\wdeIgnoredSamples.log</b> .

# Chapter 124: 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 the Web service.

Events, metrics, and topology entry points into BSM are published for external systems to use. For each event, metric, or topology that SiteScope receives, a sample is forwarded to BSM containing the event, metrics, or topology values.

## Note:

- If you are using SiteScope 11.30 or earlier, and SiteScope is connected to BSM 9.20 or later, you can only use previously created Technology Web Service Integration monitors.
- To block the creation of this monitor in the SiteScope user interface, change the `_enableEMSMonitors` property value to **false** in the `<SiteScope root directory>\groups\master.config` file, and restart SiteScope (by default, the value is set to **true**).
- For all new third-party data integrations, HPE recommends using BSM Connector. BSM Connector provides more functionality and coverage regarding the types of third-party data that can be collected than Technology Integration monitors. Note that BSM Connector works with BSM 9.20 and later only. For details on BSM Connector, see the BSM Application Administration Guide in the BSM Help.
- This monitor is not available in the user interface when using Community or Load Testing edition.

## To access

Select the **Monitors** context. In the monitor tree, right-click a group, select **New > Monitor**, and select the monitor from the New Monitor Page.

## Learn About

This section includes:

- ["Technology Web Services Overview" below](#)
- ["What Data Is Collected" on the next page](#)

## Technology Web Services Overview

SiteScope supplies a WSDL file which the user can use to create a client code. The client code reports the events, metrics, and/or topology data to SiteScope. The client has several ways to report data to BSM:

- report one event or an array of events (this is for legacy events and has been deprecated)
- report one metric or an array of metrics
- data - an array of key value pairs

## What Data Is Collected

The Technology Web Service Integration Monitor collects data that is extracted from any message received by the SiteScope Web service. The monitor processes the data, and then sends the data to BSM which contains the values selected 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 BSM. Determine if the data is for presentation in the Service Health, Service Level Management, reports, or all.

The specific data that is forwarded to BSM is controlled by the field mapping script (for script types, see Field Mapping Data Types in the Using SiteScope Guide). You use this script to specify the preferred value fields that you want forwarded. For details on the file structure and syntax, see Event Handler Structure and Syntax in the Using SiteScope Guide. For best practices and details on configuring the integration (depending on the type of sample data being captured), see How to Deploy Integration Monitors in the Using SiteScope Guide.

Data can also be mapped to a topology to forward data to the correct CI hierarchy in BSM. You can configure topology settings for the monitor by selecting one of the predefined scripts, or configuring your own topology script during monitor creation. For more details on editing the script, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.

## Tasks

### How to Integrate Data into BSM Using Web Service Entry Points

This section provides the overall flow for setting up the Technology Web Service Integration Monitor to work with BSM.

#### 1. Prerequisites

- Integration monitors are available for creation in specific instances only. For details, see the note at the top of this chapter "[Integration Monitors \(A-Z\)](#)" on page 840
- Your SiteScope must be integrated with BSM and enabled to forward data. For details on how to perform this task, see How to Configure the Integration Between SiteScope and BSM in the Using SiteScope Guide.

#### 2. Create a Technology Web Service Integration monitor

Add a Technology Web Service Integration Monitor to SiteScope. For monitor user interface details, see "[Technology Web Service Integration Monitor Settings](#)" on page 904.

#### 3. Enable the connection to the SiteScope **reportMonitorData** Web service

To enable the connection to the 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.

- a. Open a Web browser and go to SiteScope (<http://<SiteScope host>:8080/SiteScope/services/reportMonitorData?wsdl>).

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 BSM. This file is used to create the client stubs that connect to the service and report the data.

- b. 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.

- c. 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.
- d. Run your code and check if you get data in the SiteScope Technology Web Service Integration monitor.

#### 4. Use the client tool to check connectivity

After creating a Technology Web Service Integration monitor in SiteScope, you can check connectivity to the Web service by using the client check tool. This tool sends constant messages to the SiteScope **reportMonitorData** Web service from `http://<SiteScope host>:8080/SiteScope/services/reportMonitorData?wsdl`. The messages can be metrics or event messages.

- a. In the **<SiteScope root directory>\conf\ems\webservice\test\_client** directory:
  - o For events or metrics, run: **test\_data\_client.bat [Target Host][System ID]**
  - o For metrics, run: **test\_metrics\_client.bat [Target Host][Number of messages to send][System ID][Quality][Time in seconds]**
  - o For legacy events (deprecated), run: **test\_event\_client.bat [Target Host][Number of messages to send][System ID][Severity][Time in seconds]**

where:

- o **Target Host** is the address of the SiteScope host which receives the messages.
  - o **System ID** is the system ID of the monitor that receives the messages.
  - o **Number of messages to send** is the number of messages to send to SiteScope.
  - o **Quality** is the severity of metrics when forwarding metrics data (default is 0-3).
- b. If you are forwarding other values to BSM, 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 quality is 3.

If you use the option of running the test, you must activate it on the SiteScope machine and add a Technology Web Service Integration monitor with the system id: **Test Event System ID**.
  - c. After running the tool, go to the required SiteScope monitor and see if you received a message (or messages if you sent more than one message). In addition, you can access BSM and see if the data that you sent is displayed.

5. Choose one of the following reporting methods depending on the type of data you want to send:

- **For events, metrics, or topology: configure the reportData method**

**Tip:** For sending metrics data, it is recommended that you use the **reportMetricObject** and **reportMetricsArray** methods. The **reportMetricsArray** method enables you to submit metrics in bulk instead of one by one. This is a more efficient method than the **reportMetricObject** method because it involves less network traffic.

You can configure the **reportData** method while creating your SOAP message to send to SiteScope. This method contains a data structure that gets an array of key-value objects (see **DataMessage** object below).

Enter the following service request:

```
<wsdl:message name="reportDataRequest">
  <wsdl:part name="systemId" type="xsd:string" />
  <wsdl:part name="data" type="impl:ArrayOf_tns1_DataMessage" />
</wsdl:message>
```

where:

"systemId" is the unique text ID for the Technology Web Service Integration Monitor instance.

"data" is an array of any data type named **DataMessage** that contains key and value strings:

```
<complexType name="DataMessage">
  <complexContent>
    <extension base="tns1:AbstractMessage">
      <sequence>
        <element name="key" nillable="true" type="soapenc:string" />
        <element name="value" nillable="true" type="soapenc:string" />
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

The service success response is:

```
<wsdl:message name="reportDataResponse">
  <wsdl:part name="reportDataReturn" type="xsd:int" />
</wsdl:message>
```

### **Example - Sending a common event using the reportData request**

The question marks in the following example represent string values.

**Example:**

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:web="http://webservice.soa.monitors.sitescope.mercury.com"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
  <soapenv:Header/>
  <soapenv:Body>
    <web:reportData soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      <systemId xsi:type="xsd:string">?</systemId>
```

```
<data xsi:type="rep:ArrayOf_tns1_DataMessage" soapenc:arrayType="mes:DataMessage[]"
  xmlns:rep="http://localhost:8080/SiteScope/services/reportMonitorData"
  xmlns:mes="messages.client.webservice.soa.monitors.sitescope.mercury.com">
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">Title</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">Severity</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">SourceHint</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">CiHint</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">EtiHint</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">ComponentCi</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">HostHint</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">Description</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">Category</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">SubCategory</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">Key</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">CloseKey</key>
  <value xsi:type="soapenc:string">?</value>
</data>
<data xsi:type="mes:DataMessage">
  <key xsi:type="soapenc:string">LogOnly</key>
  <value xsi:type="soapenc:string">?</value>
</data>
</data>
</web:reportData>
</soapenv:Body>
```

```
</soapenv:Envelope>
```

- **For metrics: configure the reportMetricObject method**

Use the **reportMetricObject** method to submit a single metric. If you want to submit metrics in bulk, use the **reportMetricsArray** method.

Enter the following service request:

```
<wsdl:message name="reportMetricObjectRequest">
  <wsdl:part name="metric" type="tns1:MetricMessage" />
</wsdl:message>
```

where:

"metric" is one metric or an array of metrics of type `MetricMessage` that contains various value strings:

```
<complexType name="MetricMessage">
  <complexContent>
    <extension base="tns1:AbstractMessage">
      <sequence>
        <element name="measurementName" nillable="true" type="soapenc:string" />
        <element name="measurementValue" nillable="true" type="soapenc:double" />
        <element name="monitorName" nillable="true" type="soapenc:string" />
        <element name="monitorState" nillable="true" type="soapenc:string" />
        <element name="monitorType" nillable="true" type="soapenc:string" />
        <element name="quality" nillable="true" type="soapenc:int" />
        <element name="measurementETI" nillable="true" type="soapenc:string" />
        <element name="measurementCIHint" nillable="true" type="soapenc:string" />
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

The service success response is:

```
<wsdl:message name="reportMetricObjectResponse">
  <wsdl:part name="reportMetricObjectReturn" type="xsd:int" />
</wsdl:message>
```

### Example - Sending a metric using the reportMetricObject request

The question marks in the following example represent string values as follows:

- **xsd:double** is a double value
- **xsd:int** is an integer value
- **xsd:string** is a string value

#### Example:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:web="http://webservice.soa.monitors.sitescope.mercury.com">
  <soapenv:Header/>
```

```
<soapenv:Body>
  <web:reportMetricObject soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
    <metric xsi:type="mes:MetricMessage"
      xmlns:mes="messages.client.webservice.soa.monitors.sitescope.mercury.com">
      <sourceTimeStamp xsi:type="xsd:double">?</sourceTimeStamp>
      <targetName xsi:type="xsd:string">?</targetName>
      <timeStamp xsi:type="xsd:double">?</timeStamp>
      <uniqueSystemId xsi:type="xsd:string">?</uniqueSystemId>
      <measurementCIHint xsi:type="xsd:string">?</measurementCIHint>
      <measurementETI xsi:type="xsd:string">?</measurementETI>
      <measurementName xsi:type="xsd:string">?</measurementName>
      <measurementValue xsi:type="xsd:double">?</measurementValue>
      <monitorName xsi:type="xsd:string">?</monitorName>
      <monitorState xsi:type="xsd:string">?</monitorState>
      <monitorType xsi:type="xsd:string">?</monitorType>
      <quality xsi:type="xsd:int">?</quality>
    </metric>
  </web:reportMetricObject>
</soapenv:Body>
</soapenv:Envelope>
```

#### Example of field mapping script with all parameters passed by a Web Service request:

```
[$DEFAULT_PARAMETERS$]
#Any value used here will be ignored. Only the TimeStamp value passed with the web service
request is sent in the ss_t sample.
TimeStamp:DOUBLE=time()
Quality:INT=$Quality
MonitorName=$MonitorName
TargetName=$TargetName
MonitorState=$MonitorState
MonitorType=$MonitorType
MeasurementName(1)=$MeasurementName #while you can define up to four measurement names and
values in a field mapping script, only one set of name, value, ETI and CI Hint can be passed
by a web service request.
Value(1)=$Value #Note that the web service parameter name "measurementValue" is set to the
variable $Value used here.
MeasurementETI(1)=$MeasurementETI
MeasurementCIHint(1)=$MeasurementCIHint
[allR]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(ss_t)
```

#### • For metrics arrays: configure the reportMetricsArray method

The **reportMetricsArray** method enables you to submit metrics in bulk instead of one by one. This is a more efficient method than the **reportMetricObject** method because it involves less network traffic.

Enter the following service request:

```
<wsdl:message name="reportMetricsArrayRequest">
  <wsdl:part name="metrics" type="impl:ArrayOf_xsd_anyType"/>
</wsdl:message>
```

where:

"metrics" is an array of metrics of the type `ArrayOf_xsd_anyType`, which contains various value strings:

```
<complexType name="ArrayOf_xsd_anyType">
  <complexContent>
    <restriction base="soapenc:Array">
      <attribute ref="soapenc:arrayType" wsdl:arrayType="xsd:anyType[]" />
    </restriction>
  </complexContent>
</complexType>
```

## Example - Sending an array of metrics using the reportMetricsArray request

The question marks in the following example represent string values as follows:

- **xsd:double** is a double value
- **xsd:int** is an integer value
- **xsd:string** is a string value

### Example:

```
<soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:web="http://webservice.soa.monitors.sitescope.mercury.com"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
  <soapenv:Header/>
  <soapenv:Body>
    <web:reportMetricsArray soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
      <metrics xsi:type="rep:ArrayOf_xsd_MetricMessage"
        soapenc:arrayType="mes:MetricMessage[]">
        <metric xsi:type="mes:MetricMessage"
          xmlns:mes="messages.client.webservice.soa.monitors.sitescope.mercury.com">
          <sourceTimeStamp xsi:type="xsd:double">?</sourceTimeStamp>
          <targetName xsi:type="xsd:string">?</targetName>
          <timeStamp xsi:type="xsd:double">?</timeStamp>
          <uniqueSystemId xsi:type="xsd:string">?</uniqueSystemId>
          <measurementCIHint xsi:type="xsd:string">?</measurementCIHint>
          <measurementETI xsi:type="xsd:string">?</measurementETI>
          <measurementName xsi:type="xsd:string">?</measurementName>
          <measurementValue xsi:type="xsd:double">?</measurementValue>
          <monitorName xsi:type="xsd:string">?</monitorName>
          <monitorState xsi:type="xsd:string">?</monitorState>
          <monitorType xsi:type="xsd:string">?</monitorType>
          <quality xsi:type="xsd:int">?</quality>
        </metric>
        <metric xsi:type="mes:MetricMessage"
          xmlns:mes="messages.client.webservice.soa.monitors.sitescope.mercury.com">
          <sourceTimeStamp xsi:type="xsd:double">?</sourceTimeStamp>
          <targetName xsi:type="xsd:string">?</targetName>
          <timeStamp xsi:type="xsd:double">?</timeStamp>
          <uniqueSystemId xsi:type="xsd:string">?</uniqueSystemId>
          <measurementCIHint xsi:type="xsd:string">?</measurementCIHint>
          <measurementETI xsi:type="xsd:string">?</measurementETI>
          <measurementName xsi:type="xsd:string">?</measurementName>
          <measurementValue xsi:type="xsd:double">?</measurementValue>
          <monitorName xsi:type="xsd:string">?</monitorName>
          <monitorState xsi:type="xsd:string">?</monitorState>
          <monitorType xsi:type="xsd:string">?</monitorType>
          <quality xsi:type="xsd:int">?</quality>
        </metric>
      </metrics>
    </web:reportMetricsArray>
  </soapenv:Body>
</soapenv:Envelope>
```

```
</metrics>
</web:reportMetricsArray>
</soapenv:Body>
</soapenv:Envelope>
```

- **For legacy events (deprecated): configure the reportEvent method**

Enter the following service request:

```
<wsdl:message name="reportEventRequest">
  <wsdl:part name="event" type="tns1:EventMessage" />
</wsdl:message>
```

where:

"event" is one event or an array of events of type EventMessage that contains various value strings:

**Example:**

```
<complexType name="EventMessage">
  <complexContent>
    <extension base="tns1:AbstractMessage">
      <sequence>
        <element name="acknowledgedBy" nillable="true" type="soapenc:string" />
        <element name="attr1" nillable="true" type="soapenc:string" />
        <element name="attr2" nillable="true" type="soapenc:string" />
        <element name="attr3" nillable="true" type="soapenc:string" />
        <element name="attr4" nillable="true" type="soapenc:string" />
        <element name="attr5" nillable="true" type="soapenc:string" />
        <element name="dataSource" nillable="true" type="soapenc:string" />
        <element name="description" nillable="true" type="soapenc:string" />
        <element name="eventId" nillable="true" type="soapenc:string" />
        <element name="instance" nillable="true" type="soapenc:string" />
        <element name="logicalGroup" nillable="true" type="soapenc:string" />
        <element name="monitorGroup" nillable="true" type="soapenc:string" />
        <element name="object" nillable="true" type="soapenc:string" />
        <element name="origSeverityName" nillable="true" type="soapenc:string" />
        <element name="owner" nillable="true" type="soapenc:string" />
        <element name="severity" nillable="true" type="soapenc:int" />
        <element name="status" nillable="true" type="soapenc:string" />
        <element name="subject" nillable="true" type="soapenc:string" />
        <element name="targetIp" nillable="true" type="soapenc:string" />
        <element name="value" nillable="true" type="soapenc:double" />
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

The service response is:

```
<wsdl:message name="reportEventResponse">
  <wsdl:part name="reportEventReturn" type="xsd:int" />
</wsdl:message>
```

# UI Descriptions

## Technology Web Service Integration Monitor Settings

User interface elements are described below:

UI Element	Description
<b>System ID</b>	<p>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 must be unique for all monitors. Enter the system id that represents the messages that you want this monitor to receive.</p>

## Field Mapping

User interface elements are described below:

UI Element	Description
<b>Data Type</b>	<p>Select from the following data types for this integration:</p> <ul style="list-style-type: none"><li>• <b>Common Events.</b> For details, see Configuring Field Mapping for Common Event Samples in the Using SiteScope Guide.</li><li>• <b>Legacy Events.</b> For details, see Configuring Field Mapping for Legacy Event Samples in the Using SiteScope Guide.</li><li>• <b>Metrics.</b> For details, see Configuring Field Mapping for Metrics Samples in the Using SiteScope Guide.</li><li>• <b>Tickets.</b> For details, see Configuring Field Mapping for Ticket Samples in the Using SiteScope Guide.</li></ul>
<b>Load File</b>	<p>Loads the script that is applicable to the data type selected above.</p>



UI 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 BSM. To enable the integration, you must configure the mapping as required by the environment you are monitoring.</p> <p>The mapping is editable in this box using the script editor provided (you can make the script field read only by right-clicking the script and selecting <b>Configure &gt; Read Only</b>). 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 Field Mapping Data Types in the Using SiteScope Guide.</p> <p><b>Note:</b> All parameters in the field mapping should be in the format <code>logical_group</code> and not <code>logicalGroup</code>. Therefore, the target name parameter should be filled as follows:</p> <pre>target_name=resolveHostName(\$target_name)</pre>
<b>Test Script</b>	<p>Tests 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 metrics are forwarded to BSM. 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 BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Topology Settings

User interface elements are described below:

UI Element	Description
<b>Report topology without data</b>	<p>Reports the topology for the integration monitor without sending the data samples to BSM. When this option is selected, the Field Mapping panel is not available.</p> <p><b>Default value:</b> Not selected</p>

UI Element	Description
<b>Topology script</b>	<p>Script to create the topology in BSM for the samples retrieved from the monitored third-party application. The script is based on the Jython scripting language (Python enabled by Java). The monitor propagates its status to the CIs mapped in this topology. The template options displayed depend on the data type selected in the Field Mapping panel.</p> <p><b>For Event data type:</b></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 Computer or Running Software CIs.</li> <li>• <b>Computer.</b> Creates a topology with a Computer CI. Available for Common Event samples only.</li> <li>• <b>Computer - Running Software.</b> Creates a topology with a Computer CI and a Running Software CI connected to it with a <i>Composition</i> relationship. Available for Common Event samples only.</li> </ul> <p><b>Note:</b> Legacy Event samples (<b>Node</b> and <b>Node - Running Software</b>) are also available. For details, see Legacy Topology Scripts in the Using SiteScope Guide.</p> <p><b>For Metrics data type:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer - Monitor.</b> Sends the SiteScope topology with Sitescope Monitor and Computer CIs. If selected, the script area is not available.</li> </ul> <p>The <b>Computer - Monitor</b> topology integration requires that the names or IP addresses of the nodes that it adds to RTSM are accessible through DNS resolution. To successfully populate a Node CI specified in the <i>TargetName</i> field to RTSM, SiteScope must be able to resolve the node's fully qualified domain name and IP address through a DNS service.</p> <ul style="list-style-type: none"> <li>• <b>No Topology.</b> No topology is sent (although data is still sent). If selected, the script area is not available.</li> </ul> <p><b>For Tickets data type:</b></p> <ul style="list-style-type: none"> <li>• <b>Tickets.</b> Creates a Business Service CI with an EMS monitor CI connected to it with <i>Monitored By</i> relationship.</li> </ul> <p><b>Note:</b> Only select <b>Custom</b> if you are familiar with the Jython language, because you must create the topology script in Jython yourself. Depending on the data type you select, we recommend that you begin with and edit one of the predefined scripts.</p> <p>For more details, see Topology Settings for Technology Integration Monitors in the Using SiteScope Guide.</p>
<b>Load Script</b>	<p>Loads 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. The script is based on the Jython scripting language (Python enabled by Java).</p>

UI Element	Description
<b>Script</b>	<p>The contents of the script are visible in this box. You can edit the script contents in this field using the script editor provided by SiteScope, or you can copy it into your preferred text editor, edit it, and then copy it back into this box.</p> <p><b>Note:</b> The topology script is very sensitive to spaces and tabs.</p> <p>For more details on editing the script, see Editing the Topology Script in the Using SiteScope Guide.</p>
<b>Test Script</b>	<p>Tests the topology script. We recommend that you test the script before running the monitor. This test gives you the results of what events or metrics are forwarded to BSM 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: <b>&lt;SiteScope root directory&gt;\logs\bac_integration.log</b>.</p> <p><b>Note:</b> The test does not forward samples to BSM; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.</p>

## Export to BSM Connector

User interface elements are described below:

UI Element	Description
<b>Export</b>	<p>Enables exporting technology integration monitors from SiteScope and importing them to BSM Connector as policies. This feature is supported on Technology Database Integration, Technology Log File Integration, and Technology Web Service Integration monitors with a metrics, common events, or legacy events field mapping data type only.</p> <p>Select a folder on the client file system in which to save the policy files, and click <b>Open</b> to perform the export process. For task details, see Export EMS Technology Monitors to a BSM Connector Policy in the Using SiteScope Guide.</p> <p>For details on importing policies to BSM Connector, see the BSM Connector online help system (available from the toolbar of the BSM Connector user interface).</p> <p><b>Note:</b> This button is disabled and a warning message is displayed for integration monitors where export is not supported.</p>

**Note:** For information on configuring setting panels that are common to all monitors, see Common Monitor Settings in the Using SiteScope Guide.

# Troubleshooting

## Debugging Errors/Troubleshooting

This section describes troubleshooting and limitations when working with the Technology Web Service

Integration monitor.

- Check for errors in the following files:

**<SiteScope root directory>\logs\error.log**

**<SiteScope root directory>\logs\RunMonitor.log**

**<SiteScope root directory>\logs\bac\_integration\bac\_integration.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 BSM Service Health, Event Log, or SiteScope reports, look in  
**<BSM root directory>\log\wde\wdeIgnoredSamples.log** to make sure the samples were not dropped due to missing fields or values.
- Change the logging level for Service Health to verify that Service Health received the samples. Open the following file on the Gateway Server machine:

**<BSM root directory>\conf\core\tools\log4j\wde\wde.properties**

Change the log level parameter to DEBUG in the following lines:

- log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamples  
Logger=\${loglevel}, IgnoredSamples.appender
- log4j.category.com.mercury.am.platform.wde.publish\_SamplePublisher  
Samples=\${loglevel}, PublishedSamples.appender

Look at the corresponding log files:

- **<BSM root directory>\log\wde\wdeIgnoredSamples.log**

- **<BSM root directory>\log\wde\wdePublishedSamples.log**

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

## **Feedback on Monitor Reference (SiteScope 11.32)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [sitescope-doc-feedback@hpe.com](mailto:sitescope-doc-feedback@hpe.com).

We appreciate your feedback!