HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 7.0

Using System Availability Management

Document Number: BACSAM7.0/01

Document Release Date: February 2008

Software Release Date: August 2007

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Third-Party Web Sites

HP provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. HP makes no representations or warranties whatsoever as to site content or availability.

Copyright Notices

Trademark Notices

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

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

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

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

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

Unix® is a registered trademark of The Open Group.

Documentation Updates

This manual's title page contains the following identifying information:

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

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

http://ovweb.external.hp.com/lpe/doc_serv/

Support

Mercury Product Support

You can obtain support information for products formerly produced by Mercury as follows:

- If you work with an HP Software Services Integrator (SVI) partner (**http://h20230.www2.hp.com/svi_partner_list.jsp**), contact your SVI agent.
- If you have an active HP Software support contract, visit the HP Software Support Web site and use the Self-Solve Knowledge Search to find answers to technical questions.
- For the latest information about support processes and tools available for products formerly produced by Mercury, we encourage you to visit the Mercury Customer Support Web site at: **http://support.mercury.com**.
- If you have additional questions, contact your HP Sales Representative.

HP Software Support

You can visit the HP Software Support Web site at: **www.hp.com/go/hpsoftwaresupport**

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To find more information about access levels, go to:
http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:
http://h20229.www2.hp.com/passport-registration.html

Table of Contents

PART I: SYSTEM AVAILABILITY MANAGEMENT

PART II: SITESCOPE GENERAL AND ADMINISTRATION

PART III: SITESCOPE DASHBOARD

PART IV: MONITORS

PART V: INTEGRATION MONITORS

PART VI: TEMPLATES

PART VII: ALERTS AND REPORTS

PART VIII: SITESCOPE ADVANCED INFORMATION

Welcome to This Guide

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

How This Guide Is Organized

The guide contains the following parts:

Part I System Availability Management

Describes how to use System Availability Management Administration from within HP Business Availability Center to register, configure, and maintain multiple SiteScopes. It also describes using the Monitor Deployment Wizard and System Availability Management reports.

Part II SiteScope General and Administration

Describes the SiteScope's general and administrative functions, including the monitor tree, preferences, Views and Categories, and the Global Search and Replace Wizard.

Part III SiteScope Dashboard

Describes how to use the SiteScope Dashboard tab to view the latest real-time monitor data and to customize the display of monitor results.

Part IV Monitors

Describes how to configure each type of SiteScope monitor.

Part V Integration Monitors

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

Part VI Templates

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

Part VII Alerts and Reports

Describes how to use SiteScope Alerts to send notifications of an event or change of status in your infrastructure, and how to generate SiteScope Reports to define the monitor parameters, time interval, or summary data you want to measure.

Part VIII SiteScope Advanced Information

Describes how to use regular expressions, monitor XML documents, write script alerts, customize alert templates, create and customize adapter files for UNIX monitoring, use Secure Shell (SSH) connection for remote server monitoring, configure clients working with SSH, customize monitor properties, and use SiteScope tools to troubleshoot and diagnose resource and monitor configuration problems.

Who Should Read This Guide

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

- HP Business Availability Center administrators
- HP Business Availability Center application administrators
- HP Business Availability Center data collector administrators
- HP Business Availability Center 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 should be familiar with HP Business Availability Center and enterprise monitoring and management concepts.

Getting More Information

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

Part I

System Availability Management

1

System Availability Management Administration

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

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

System Availability Management Administration Overview

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

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

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

System Availability Management enables you to:

- Add SiteScopes to System Availability Management Administration. For details, see "New SiteScope Page" on page 47.
- Copy group, monitor, report, and alert instances from one SiteScope to another SiteScope using copy/paste. For details, see "Copying and Moving SiteScope Objects" on page 149.
- Synchronize a SiteScope's settings with another SiteScope by copying settings, preferences, and template files using the Synch SiteScope wizard. For details, see "Sync SiteScopes Wizard" on page 50.
- Perform a Global Replace operation across multiple SiteScopes. For details, see "Global Search and Replace Wizard" on page 279.

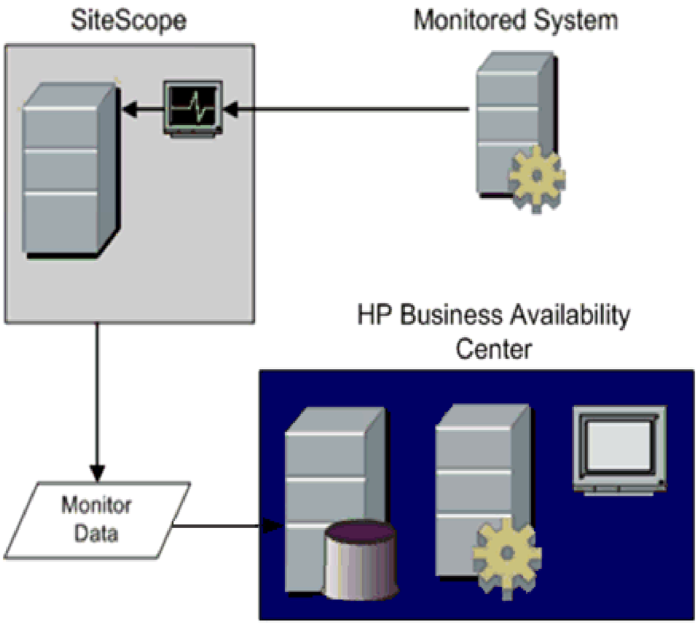
- View accessibility information and summary information regarding registration status of the SiteScope to Business Availability Center, licence points, sample reporting rates, monitor run rates and health of the SiteScopes. For details, see "System Availability Management Administration" on page 40.
- Run the Monitor Deployment Wizard to deploy monitors onto configuration items in Business Availability Center's CMDB. For details, see "Monitor Deployment Wizard Concepts and Tasks" on page 59.

Understanding SiteScope Integration with HP Business Availability Center

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

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

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



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

There are two main aspects of compatibility between SiteScope and HP Business Availability Center. The first is data logging which is the process of logging data collected by SiteScope to HP Business Availability Center for the purposes of real-time status, reporting, Service Level Management, and so forth. The second aspect of compatibility is System Availability Management Administration which refers to configuring SiteScope (including deploying monitors) from within HP Business Availability Center.

The following table contains compatibility information regarding these two aspects and the various combinations of SiteScope and HP Business Availability Center releases.

- 1 = Data logging support
- 2 = Configuration support
- X = Not supported

SiteScope Version	**HP Business Availability Center Version**					
	7.0	**6.5**	**6.1**	**6.0**	**5.1**	**5.0**
SiteScope 9.0	1,2	1	1	1	1	1
SiteScope 8.5	1	1,2	1,2	1,2	1,2	1
SiteScope 8.2	1	1,2	1,2	1,2	1,2	1
SiteScope 8.1.2 (recommended version for 6.1)	1	1,2	1,2	1,2	1,2	1
SiteScope 8.1, 8.1.1	1	1,2	1,2	1,2	1,2	1
SiteScope 8.0 SP2	1	1,2	1,2	1,2	1,2	1
SiteScope 8.0, 8.0 SP1	1	1	1	1	1,2	1
SiteScope 7.9.5.x	1	1,2	1,2	1,2	1,2	1
SiteScope 7.9.1.0	1	1	1	1	1	1,2
SiteScope 7.9.0.0	1	1	1	1	1	1
SiteScope 7.8.1.0, 7.8.1.2	X	X	X	X	1	1

When SiteScope is registered as a data collector reporting data to HP Business Availability Center, it may also be accessed as a standalone product.

Accessing SiteScope and Building Permissions Model

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

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

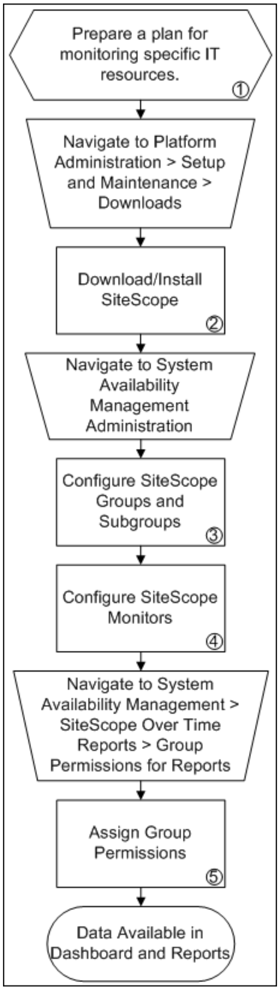
There are several differences between the Business Availability Center permissions model and SiteScope standalone permissions:

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

  For example, a user can have permissions within Business Availability Center to view or change specific instances of SiteScope groups with no permission to access other SiteScope groups.
- SiteScope enables specific types of permissions onto object types, such as the ability to enable/disable whereas in Business Availability Center the operations are standard for all objects and include view, change, add, and full control. In this case, enable/disable is mapped to Business Availability Center's change permission.
- When applying permissions in Business Availability Center onto SiteScope objects, you can hover over an operation to see a description of how it maps to the permissions available to user's of SiteScope standalone.
- Only a user at the Administrator level in SiteScope standalone has the necessary permissions to add a SiteScope to System Availability Management Administration in Business Availability Center.

Collect Data on the Performance of an IT Resource

The flowchart below describes the process required to set up and use SiteScope to collect data on the performance of IT infrastructure components. The numbered elements are referenced in the table on the following page, which provides additional details about the steps and a reference to more information.


Prepare a plan for monitoring specific IT resources.
①
Navigate to Platform Administration > Setup and Maintenance > Downloads
Download/Install SiteScope
②
Navigate to System Availability Management Administration
Configure SiteScope Groups and Subgroups
③
Configure SiteScope Monitors
④
Navigate to System Availability Management > SiteScope Over Time Reports > Group Permissions for Reports
Assign Group Permissions
⑤
Data Available in Dashboard and Reports

Ref. No.	Comment
1	Prepare a plan that maps out the specific IT infrastructure resources about which you want to collect data. Include information about the business processes that are affected by the specified infrastructure components (for example, business processes—being monitored by Business Process Monitor—that are running on an application server against which you plan to run SiteScope monitors).
2	Download and save the SiteScope installation files (for Windows or Solaris) to a local or network drive. Install SiteScope on machines designated to run the SiteScope data collector. You can run multiple SiteScopes from multiple platforms. For more information, see the *HP SiteScope Deployment Guide* PDF.
3	Add the SiteScope to System Availability Management Administration and configure the SiteScope's Business Availability Center preferences. For details, see "New SiteScope Page" on page 47, and "HP Business Availability Center Preferences" on page 233. Create groups and subgroups to organize the monitors to be deployed. For example, you can create groups of locations, server types, network resources, and so forth. For more information, see "SiteScope Group Settings" on page 617.
4	When configuring monitors, verify that HP BAC Logging settings are set as required. You can use the Monitor Deployment Wizard to deploy monitors onto existing CIs in the CMDB. You can also use Solution Templates to configure predefined sets of monitors on specific systems. For more information, see "SiteScope Solution Templates Overview" on page 1073. Once defined, the SiteScope and its groups and monitors are added as CIs to the CMDB and are automatically attached to the relevant monitor views, from where they can be added to other views. During monitor configuration, you can associate the monitor with existing CIs using Link Monitor to CI Settings (for example you can attach the CPU monitor to an existing logical CI representing a machine whose CPU is being monitored). The data from the SiteScope is available in Dashboard and Service Level Management.
5	For each defined user, assign permissions to view SiteScope groups and their subgroups in System Availability Management reports and custom reports. For more information, see "Set Group Permissions for Reports" on page 126.

Troubleshooting System Availability Management Administration

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

Possible Solution: Add the SiteScope machine's URL to trusted sites in Internet Explorer's options and restart all browsers.

Reverse integration does not work.

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

Page can not be displayed due to 404 error.

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

Possible Solution: Check your DNS settings.

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

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

Possible solution: Install flash on the client browser.

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

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

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

2

System Availability Management Administration User Interface

This chapter includes a description of the pages and dialog boxes that are part of the System Availability Management user interface.

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

System Availability Management Administration

Description	System Availability Management Administration is a portal within HP Business Availability Center that enables you to add SiteScope servers to an HP Business Availability Center system and to access those SiteScope servers. The SiteScopes are represented as nodes in the tree in the left pane. ➤ When you highlight the root node, the right pane displays the System Availability Management features, including summary information for the SiteScopes. ➤ When you highlight a SiteScope in the tree, the right pane displays that SiteScope's Dashboard and you can perform any function within the SiteScope. **To access**: Select **Admin** > **System Availability Management**.
Important Information	Each SiteScope is listed by name with an icon displaying its current connection status to BAC. You access the SiteScope server by highlighting the name of the server in the list in the left pane.

The System Availability Management Administration page includes the following sections:

List of SiteScope Servers - Left Pane

GUI Element	Description
<SiteScope server name>	Represents an individual SiteScope server. The name includes a tooltip that displays the following data: ➤ **Health**. Health status of the SiteScope server represented by a status icon. ➤ **Mode**. Whether the SiteScope is currently hosted by the HP Business Availability Center. ➤ **Points**. The number of license points in use by the SiteScope. ➤ **Remote server**. The number of remote servers being monitored by this SiteScope. ➤ **Operating system**. The type of OS on which the SiteScope is running. ➤ **High Availability server**. The name of the server used by this SiteScope for failover.
🖥✓	Icon accompanying the SiteScope name indicating that the SiteScope is registered to HP Business Availability Center and fully accessible from System Availability Management Administration. A SiteScope with this status is considered ‘hosted’ by HP Business Availability Center.
🖥🚫	Icon accompanying the SiteScope name indicating that the SiteScope is registered to HP Business Availability Center but not available for configuring. A SiteScope with this status reports data to HP Business Availability Center but can be configured only when accessing the SiteScope standalone.
🖥□	Icon accompanying the SiteScope name indicating that the existing SiteScope profile is empty and there is no running SiteScope associated with it.

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

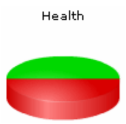
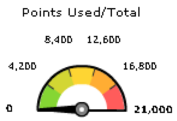
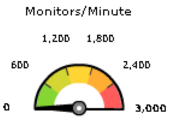
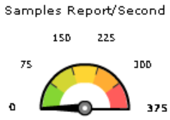
Context Menu Options

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

Summary Information - Right Pane

Description	When you highlight the root node, the right pane displays the summary information for all the SiteScopes accessed by this HP Business Availability Center. **To access**: Select **Admin** > **System Availability Management** and highlight the root node in the left pane.
Important Information	You access the SiteScope server by highlighting the name of the server in the list in the left pane or by clicking the name of the SiteScope in the table. The graphs displayed at the top of the page are a summary of all the SiteScopes listed.

The right pane includes the following elements:

GUI Element	Description
	Graph represents the overall health status of the listed SiteScopes. Each SiteScope represents its proportionate section of all the SiteScopes attached to HP Business Availability Center.
	Gauge represents the current monitor points that are in use by all the registered and configurable (hosted) SiteScopes versus the total points available for this installation.
	Gauge represents the total runs per minute and is calculated by taking the sum of all monitor runs per minute for all the hosted SiteScopes versus the number of hosted SiteScopes times 1000 (the maximum number of monitor runs per minute).
	Gauge displaying the rate of samples being reported from all SiteScopes to HP Business Availability Center. The maximum number of samples per second is determined by the HP Business Availability Center deployment.

GUI Element	Description
▤	You can adjust the width of the table's columns by dragging the borders of the column to the right or the left. Click to reset the table columns' width to its default setting.
▥	Click to open the Select Columns dialog box and select the columns you want displayed in the table.
Global Search and Replace	Click to open the Global Search and Replace Wizard to update properties across multiple SiteScopes. For details, see “Global Search and Replace Wizard” on page 279.
Sync SiteScopes	Click to open the Sync SiteScope Wizard to copy preferences, settings, and configuration files between SiteScopes. For details, see “Sync SiteScopes Wizard” on page 50.

SiteScope Summary Table

Table Column	Description
Display Name	The name give to the SiteScope when it was added to System Availability Management Admin.
Points Used/Total	The number of license points currently being used by the SiteScope versus the total license points available.
Deployed Monitors	The number of monitors configured the specific SiteScope server.
Monitors/Minute	The number of monitor runs per minutes.
Remote Targets	Displays the number of remote servers being monitored by this SiteScope.
OS	The operating system on which the SiteScope is running.
Version	The version of the SiteScope software.
Samples/Report	Displays the rate of samples reported from this SiteScope to HP Business Availability Center.

Table Column	Description
HA Status	Displays whether the failover SiteScope installation is running or not and whether the failover SiteScope is running instead of the primary SiteScope.
Health	Indicates the status of the SiteScope itself. The following are the available status levels: 🟢 **OK**. All performance measurements are within the OK threshold level. 🟡 **Warning**. At least one performance measurement is within the Warning range, but no measurements are within the Error or Poor range. 🔴 **Error/Poor.** At least one performance measurement is within the Error or Poor range. This indicates either of the following: ➤ the performance measurement has a value, but at poor quality level ➤ there is no measurement value due to some error ⚪ **No thresholds breached.** No thresholds were defined for the monitor, so no status is assigned.
MDW	Click to access the Monitor Deployment Wizard. You use the wizard to deploy monitors from the SiteScope onto existing CIs in HP Business Availability Center. For details, see "Monitor Deployment Wizard Concepts and Tasks" on page 59.

Optional Columns for SiteScope Summary Table

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

New SiteScope Page

Description	Use to add an existing SiteScope to this HP Business Availability Center. You can determine whether the SiteScope is hosted by System Availability Management or if it just reports data to HP Business Availability Center.
Important Information	Once a SiteScope is added to the System Availability Management page, it is assigned a connectivity status. Only a user who is defined with Administrator permissions in SiteScope standalone can add that SiteScope to System Availability Management Administration.
Useful Links	"System Availability Management Administration" on page 40

The New SiteScope Page includes the following areas:

Main Settings

GUI Element	Description
Display Name	Enter a descriptive name representing this SiteScope in System Availability Management Admin. This name identifies the SiteScope in the list of SiteScopes in the left pane and in the summary list in the right pane.
Host Name	Enter the host name or IP address of the machine on which SiteScope is currently running.

GUI Element	Description
Port Number	Enter the port number used to communicate with SiteScope. **Default:** 8080
Inaccessible Profile	Use this field to create a profile for a SiteScope that is not currently accessible from HP Business Availability Center. Creating the profile in this way adds the profile name to the database but there is no connection to the SiteScope from HP Business Availability Center until the actual registration from SiteScope. **Example:** Enter a profile name for a SiteScope to report data to HP Managed Software Solutions. HP Managed Software Solutions cannot access the SiteScope until it has been registered from the SiteScope.

Distributed Settings

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

Advanced Settings

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

Profile Settings

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

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

Sync SiteScopes Wizard

Description	Use this wizard to synchronize settings from different SiteScopes by copying files and settings from one SiteScope to another. **To Access:** Select **Admin** > **System Availability Management** and click **Sync SiteScopes**.
Important Information	This wizard can be used to copy the settings configured for a SiteScope to another SiteScope. To copy groups, monitors, alerts, or reports from one SiteScope to another SiteScope, use the **Copy** and **Paste to another SiteScope** option in the monitor tree's context menu.
Wizard Map	The Sync SiteScopes wizard includes: Select Source and Targets Page > Select Types to Sync > Select Instances to Sync.

Select Source and Targets Page

Description	Use this page to select the source SiteScope from which to copy settings and the target SiteScope to which to copy settings.
Important Information	This page lists only those SiteScopes that: ➤ are version 9.0 or higher ➤ have been added to System Availability Management ➤ are currently accessible to HP Business Availability Center
Wizard Map	The Sync SiteScopes wizard includes: **Select Source and Targets Page** > Select Types to Sync > Select Instances to Sync.

The page includes the following elements:

GUI Element	Description
Source SiteScope	Select the SiteScope from which to copy settings or files. You can select only one SiteScope from which to copy. Once a SiteScope is selected as the source, it cannot be selected as a target. **Note:** Only those SiteScopes appear for which the current user has at least view permissions as applied in Permissions Management. For details, see "Understanding Roles and Operations" on page 320.
Target SiteScope	Select the SiteScopes to which to copy settings or files. You can select multiple SiteScopes as the target of the synchronization. **Note:** Only those SiteScopes appear for which the current user has at least change permissions as applied in Permissions Management. For details, see "Understanding Roles and Operations" on page 320.
☑ ☐ ⇄	You can use these options to select all listed SiteScopes, clear the selection, or invert the current selection. These options apply only to the **Target SiteScope**.

Select Types to Sync

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

SiteScope Objects

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

GUI Element	Description
Preferences	Copy the preferences configured in the source SiteScope to the target SiteScope. Only those preferences that have been configured in the source SiteScope appear here. If no preferences or instances of preference types have been defined in the source SiteScope, there are no preferences listed here. The following preferences can be selected for the sync operation: ➤ E-mail preferences ➤ Pager preferences ➤ SNMP trap preferences ➤ Absolute schedule preferences ➤ Range schedule preferences For details on types of preferences, see “Preferences” on page 181. **Example**: Copy the absolute schedules that have been configured in the source SiteScope to the target SiteScope. You can then use those same absolute schedules when scheduling monitors to run (while configuring or editing monitors) in the target SiteScope.

GUI Element	Description
Categories	Copy the categories configured in the source SiteScope to the target SiteScope. If no categories have been defined in the source SiteScope, there are no categories listed here. For details about using categories in SiteScope, see "Working with Categories" on page 173. **Example**: A category defining operating system with values of Windows, Linux, and so forth has been defined in the source SiteScope. These same categories can be copied for use in the target SiteScope.
Templates	Copy the templates configured in the source SiteScope to the target SiteScope. If no templates have been defined in the source SiteScope, there are no templates listed here. For details about working with templates in SiteScope, see "Using SiteScope Templates" on page 1039.

SiteScope Files

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

GUI Element	Description
SNMP Template Files	Templates that can be selected when creating an SNMP trap alert action. Select to copy all the files in the following folder path: **<SiteScope root directory>/templates.snmp**.
Certificate Template Files	Select to copy all the files in the following folder path: **<SiteScope root directory>/templates.certificates**.
Post Template Files	Templates that can be selected when creating a post alert action. Select to copy all the files in the following folder path: **<SiteScope root directory>/templates.post**.
OS Template Browsable Files	Select to copy all the files in the following folder path: **<SiteScope root directory>/templates.os/browsable**.

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

Select Instances to Sync

Description	This page displays a tree with all the instances of the type of file or object selected in the Select Types to Sync page. You can then select specific instances of the file type or object type you want copied from the source SiteScope to the target SiteScopes.
Important Information	You can use the **Select All**, **Clear Selection**, and **Invert Selection** buttons to modify your selection of file or object instances. When you finish making your selections, click **Finish** and the Summary page opens indicating the number of objects or files successfully copied to the target SiteScopes.
Wizard Map	The Sync SiteScopes wizard includes: Select Source and Targets Page > Select Types to Sync > **Select Instances to Sync**.

The page includes the following elements:

GUI Element	Description
<Files/objects tree>	Use the tree to select or clear specific instances occurring in the source SiteScope of the file type or object type you want to copy to the target SiteScope. The tree lists all instances of the selected file type or object type that occur in the source SiteScope. **Default**: All instances of every file or object selected in the Select Types to Sync page are selected. Clear the check box next to an instance to remove it from the sync operation.
Override existing instances	Select this option for the sync action to override any instances of the same name in the target SiteScopes with the selected instances. If this option is cleared and during the sync operation, an instance of the object or type with the same name is found in the target, the sync operation does not copy the instance onto the target SiteScope. **Example**: You selected Absolute Schedule Preferences in the Select Type to Sync page and the target SiteScope has an absolute schedule with the same name as in the source SiteScope: ➤ If this option is selected, the target's absolute schedule is overwritten with the properties of the schedule in the source SiteScope. ➤ If this option is cleared, the target's absolute schedule maintains its properties and is not overwritten.

3

Monitor Deployment Wizard Concepts and Tasks

This chapter includes the main concepts, tasks and reference information for the Monitor Deployment Wizard.

Note: The Monitor Deployment Wizard is available only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center.

Overview of the Monitor Deployment Wizard

The Monitor Deployment Wizard provides a monitoring solution for existing Business Availability Center configuration item (CI) data using SiteScope templates. The wizard uses SiteScope templates to deploy monitors, groups, and remote servers with the existing and discovered CI data from the CMDB. For details on understanding CIs, see “Configuration Management Database (CMDB) Concepts” in *Reference Information*.

SiteScope templates enable you to deploy group and monitor configurations across multiple infrastructure elements with a minimal number of configuration steps. For details, see “Using SiteScope Templates” on page 1039.

The Monitor Deployment Wizard uses SiteScope’s template functionality to create a monitoring solution for the CIs in your CMDB. When you select CIs to monitor using the Monitor Deployment Wizard, the wizard automatically matches templates to the selected CIs based on the CI type selected. You can also select additional templates to apply to the selected CIs for your specific monitoring requirements. For details on which templates are deployed onto which CI types, see “Template Reference” on page 74.

The CMDB may already include CI data that can be used for monitor deployment. These properties may have been entered while adding the CI to the IT Universe model or may have been discovered by the Discovery Manager. For details, see “Populate an Instance View” in *IT World Model Management*. The wizard is also able to retrieve the data from the CMDB for the selected CIs and use that data when deploying the SiteScope templates.

HP Business Availability Center enables you to use that data to create SiteScope monitors, groups, and remote servers for existing CIs in the CMDB.

The Monitor Deployment Wizard:

- enables you to select CIs onto which to deploy the SiteScope templates
- recognizes the CIs onto which a SiteScope monitor can be deployed
- recognizes which templates to deploy onto which CIs
- enables you to refine the selection of templates to deploy onto CIs

- checks the CI for existing monitors and measurements that match the monitoring solution to be deployed by the template and enables you to handle duplicate monitoring
- imports the configuration item's properties that have been defined in CMDB Administration into the monitor's properties and creates remote servers on SiteScope
- uses template variables to enable you to enter data for monitor properties that are not imported from the configuration item's definition
- creates in the CMDB a **monitored by** relationship between the monitored CI and the created monitor

Example of Monitor Deployment

For example, an Oracle database has been added as a CI to the IT Universe model in CMDB Administration. You can use the Monitor Deployment Wizard to deploy the Oracle Database monitor onto the CI. The wizard imports the following properties that are defined for the server in the CMDB:

- database server IP address or server name
- database user name
- database password
- database port
- database SID

If a partial Discovery was run during the Discovery process, the wizard prompts you to enter values for some of the variables that are necessary for the deployment of the monitors.

Prerequisites for Running the Monitor Deployment Wizard

Before running the Monitor Deployment Wizard, you need to run the relevant discovery jobs to discover CIs and populate views. For details on the Discovery process, see “Discovery Overview” in *Discovery*.

After you have discovered the relevant CIs in your business environment, you can select one of the pre-defined views populated by the Discovery jobs. Alternatively, you can create a view manually for the purpose of running the Monitor Deployment Wizard. It is recommended to create a **Host Credentials** view which contains hosts with credentials. This can help to streamline the process of selecting the relevant hosts to be monitored in the Select CIs to Monitor step of the wizard.

To create a Host Credentials view:

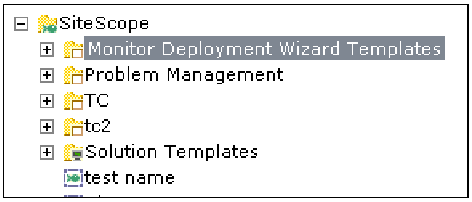
1. Select **Admin** > **Universal CMDB** > **Modeling** > **View Manager**.
2. From the Views pane, right-click the Root folder in the tree.
3. Select **New** from the context menu. The Create New View dialog box opens.
4. Enter Host Credentials in the View Name window.
5. From the CI Types pane, expand the System branch of the tree. Click and drag the Host CI type into the Editing pane.
6. From the CI Types pane, expand the Software Element branch of the tree. Click and drag the Shell CI type into the Editing pane.
7. Holding down the CTRL key, select both the Host and Shell nodes in the Editing pane. Right-click one of them and select **Add Relationship**. The Add Relationship dialog box opens.
8. In the Add Relationship dialog box, click **Advanced**. Select **Container Link** from the tree in the relationship window. Click **OK**.
9. Right-click the shell node in the Editing pane and select **Node Condition** from the context menu. The Node Condition dialog box opens.
10. In the Node Condition dialog box, clear the **Visible** check box and click **OK**.
11. Click the **Save** button from the toolbar to save the view.

For details on creating views, see “Create New View/View Properties Dialog Box” in *IT World Model Management*.

Note: In the Select CIs to Monitor step of the wizard, you can select CIs to monitor from many different views, but a specific CI may be selected only once, even if it appears in more than one view.

Monitor Deployment Wizard Templates and Variables

The Monitor Deployment templates appear by default in the monitor tree in a container called **Monitor Deployment Wizard Templates**. This container and the templates and variables within it should not be edited or deleted.



- SiteScope
  - Monitor Deployment Wizard Templates
  - Problem Management
  - TC
  - tc2
  - Solution Templates
  - test name

Only advanced users with a thorough knowledge of working with templates should attempt to edit any of the variables or to add variables to the templates. For details, see “Using SiteScope Templates” on page 1039.

Monitor Template Variables

The templates associated with the selected CIs have variables which must be filled in before the wizard can deploy them. The system fills in most of the variables automatically by checking the CI information or the results of the Discovery process. Other variables are not filled in by the system because the data was missing from the CI information, the Discovery process did not run completely, or because the data is dependent on the user. You must fill in the missing information for any selected monitor templates. You also have the option of not deploying the template by clearing the template selection if you do not know the variable values.

Selecting Templates

Once a CI is selected, all the relevant templates are matched to the CI.

In the step for entering variable values, a check box appears next to each monitor template associated with that CI. By default, if there is any missing data for the variables in a template, that template is not selected for deployment. This enables the wizard to streamline the deployment process.

You can select or clear templates for deployment. If you select a template for deployment but fail to enter the missing data for its variables, an error message appears and the wizard cannot proceed until you enter the data. If you leave any templates unselected, a warning message appears to alert you that there are unselected templates but you can choose to proceed with the wizard anyway. This applies to all unselected templates, whether data was entered for them or not.

Manual Template Matches

The wizard enables you to select other templates for deployment that were not automatically mapped by the wizard. For example, you may want to use an existing template that includes log file monitoring that is set to search for a specific string that would be relevant for host CIs in your environment. You can choose to deploy that template onto the host CIs you selected in the Select CIs to Monitor page.

You may also want to select a CI type that does not have a template associated with it and deploy an existing template onto that CI.

If you have matched additional monitor templates to be deployed onto CI types that are not in those predefined in the wizard, you can save these matches for future use when the same Business Availability Center user runs the wizard.

Also, if you removed templates that were matched by the wizard for specific CIs and chose to save matching, those templates are not matched to the selected CIs the next time the same Business Availability Center user runs the wizard.

For details, see "Save Matching" on page 88.

Full and Partial Monitor Coverage

For each selected CI, the Monitor Deployment Wizard checks whether the CI already has a monitored by relationship with any monitor CIs that are equivalent to the monitor instances that would result from the wizard deploying the templates mapped for that CI. It further checks the actual measurements within the monitor CIs and determines if the monitoring solution deployed by the wizard duplicates the monitors that exist for the selected CI.

If the CI onto which you want to deploy the monitoring solution already contains all of the same monitor and measurement instances, the CI is considered **fully covered**. If the CI has only part of the monitors and measurements already deployed, the CI is considered **partially covered**.

You can choose to clear fully or partially covered CIs and disable them for the deployment. Or, you have the option of continuing with the deployment and handling the duplicate monitors in the final step of the wizard. If, in the final step of the wizard, duplicate monitors on CIs were detected and the wizard successfully deployed templates onto these CIs, a **Handle Duplicates** button is displayed and enables you to delete these monitors, disable them or leave them in tact as duplicated monitors.

Wizard Options

CI Group Hierarchy Option

When you deploy templates using the Monitor Deployment Wizard, you can choose to create a CI group hierarchy which mirrors the CI hierarchy in the selected view in HP Business Availability Center. This means that SiteScope groups are created to correspond to the parent and grandparent CIs of the CI being monitored. These groups are arranged in a tree structure identical to the one that contains the actual CIs in the selected view in HP Business Availability Center.

SiteScope Remote Preferences

The SiteScope templates used in the Monitor Deployment Wizard are configured with template remotes which create remote server preferences in SiteScope for use by other SiteScope monitors. The remote servers created can be found in SiteScope under **Preferences** > **Windows Remote Preferences** (for Windows monitors) and **Preferences** > **Unix Remote Preferences** (for UNIX monitors). For details on remote preferences, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.

When the wizard deploys a template with remote server definitions for a physical monitor (for example, a CPU monitor), a remote preference is created with the name of the host (the host DNS name) plus the username. When deploying a template with a remote server that already exists in SiteScope's remote preferences, SiteScope uses the existing remote and does not create another remote preference. For details creating remote preferences with templates, see "Template Remotes" on page 1053.

Reporting

The final step of the Monitor Deployment Wizard consists of the Deployment Results page which displays information about the successful and unsuccessful monitor deployments. The report contains the names of the selected CIs and the monitors selected for deployment. The deployment status is indicated for each monitor.

The report can be exported to a PDF or a CSV file. These reports include detailed information displaying all the created groups, monitors, and alerts, including the exact location where they can be found in SiteScope. These reports are useful for large deployments. For example, when hundred of CIs are selected in the wizard, the resulting deployment can include thousands of new objects added to the SiteScope. For details, see "Deployment Results Page" on page 91.

Note: After running the Monitor Deployment Wizard, the deployed monitors are not run immediately, but rather within the defined frequency scheduled for the monitor.

Monitor Deployment Wizard for Siebel

You can use the Monitor Deployment Wizard to monitor your Siebel environment. The view to use for the wizard is the **Siebel Enterprise** view. The wizard can identify the Siebel configuration items in the CMDB and deploy a set of pre-configured monitors onto those items. The monitors include those that are specifically designed to monitor Siebel, as well as generic monitors that can monitor the performance of your Siebel network.

For details on the available templates used for the Siebel environment, see "Siebel Solution Templates" on page 1131.

For reference information on the Siebel monitor template and configuration items, see "Template Reference for Siebel" on page 77.

Deploy Monitors Using the Monitor Deployment Wizard

To deploy monitors using the Monitor Deployment wizard, proceed according to the following workflow:

Run Discovery

Prior to deploying monitors with the Monitor Deployment Wizard, you must discover the CIs in your system and populate views.

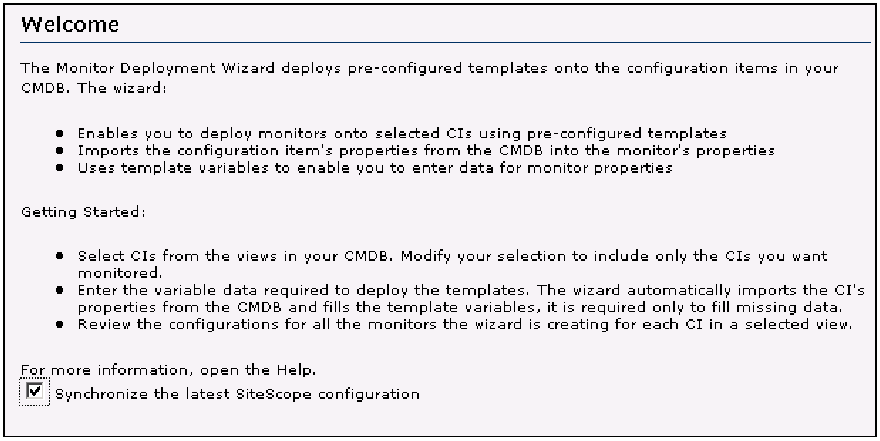
It is recommended that you create a Host Credentials view for the purpose of running the Monitor Deployment Wizard. For details, see "Prerequisites for Running the Monitor Deployment Wizard" on page 62. While this is not mandatory, it is recommended so that the necessary credentials exist to access the servers.

Begin Running the Wizard

Run the first two steps of the wizard. For details, see "Monitor Deployment Wizard" on page 84. These steps include synchronizing SiteScope data and selecting CIs to monitor using the View Explorer. For details, see "Select CIs to Monitor Page" on page 86.

After selecting CIs to monitor, you can select monitor templates to apply to them using the Templates Selection dialog box. For details, see "Templates Selection Dialog Box" on page 87.

Example:



Welcome

The Monitor Deployment Wizard deploys pre-configured templates onto the configuration items in your CMDB. The wizard:

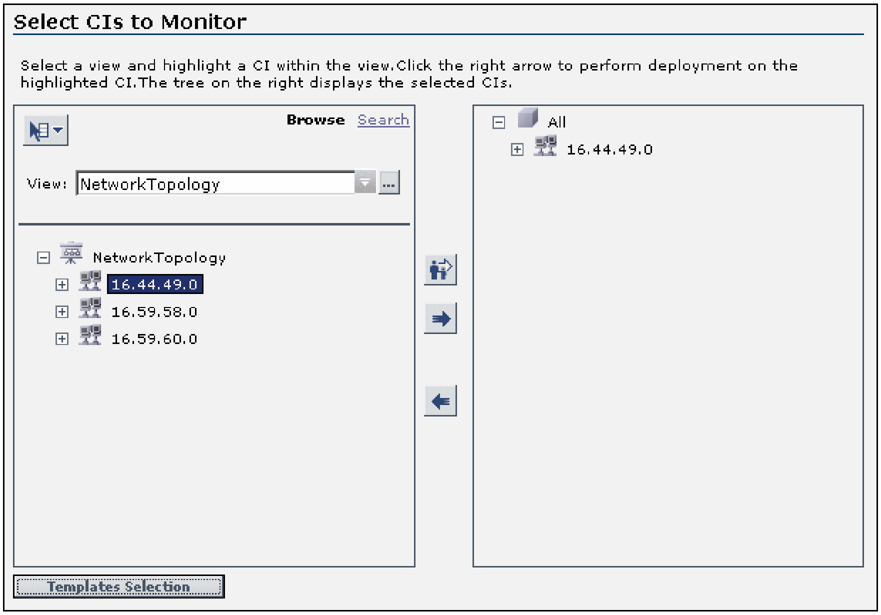
- Enables you to deploy monitors onto selected CIs using pre-configured templates
- Imports the configuration item's properties from the CMDB into the monitor's properties
- Uses template variables to enable you to enter data for monitor properties

Getting Started:

- Select CIs from the views in your CMDB. Modify your selection to include only the CIs you want monitored.
- Enter the variable data required to deploy the templates. The wizard automatically imports the CI's properties from the CMDB and fills the template variables, it is required only to fill missing data.
- Review the configurations for all the monitors the wizard is creating for each CI in a selected view.

For more information, open the Help.

☑ Synchronize the latest SiteScope configuration



Select CIs to Monitor

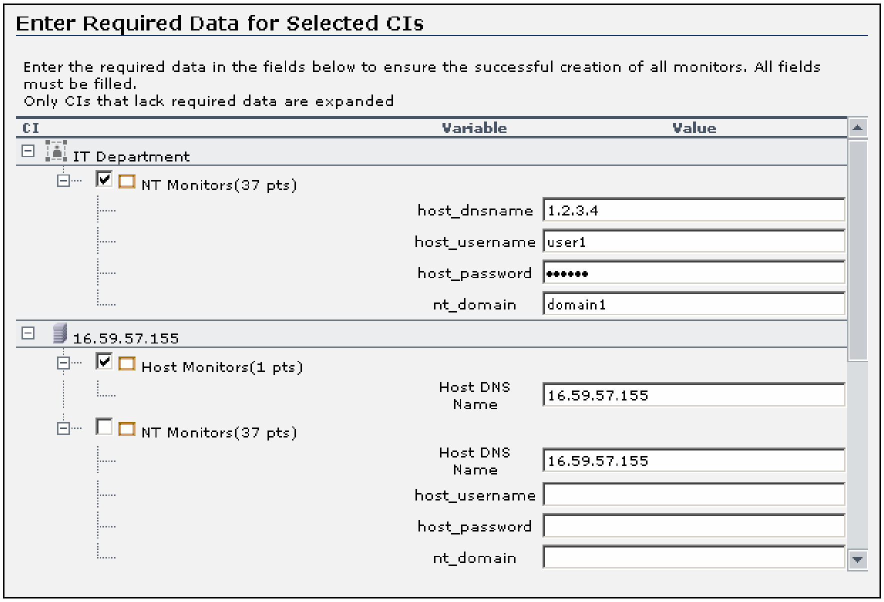
Select a view and highlight a CI within the view.Click the right arrow to perform deployment on the highlighted CI.The tree on the right displays the selected CIs.

View: NetworkTopology

Enter Missing Data for Selected CIs

On the third page of the wizard, select the monitor templates to deploy and enter any missing data for them. For details, see “Enter Required Data for CIs Page” on page 89.

Example:



Enter Required Data for Selected CIs

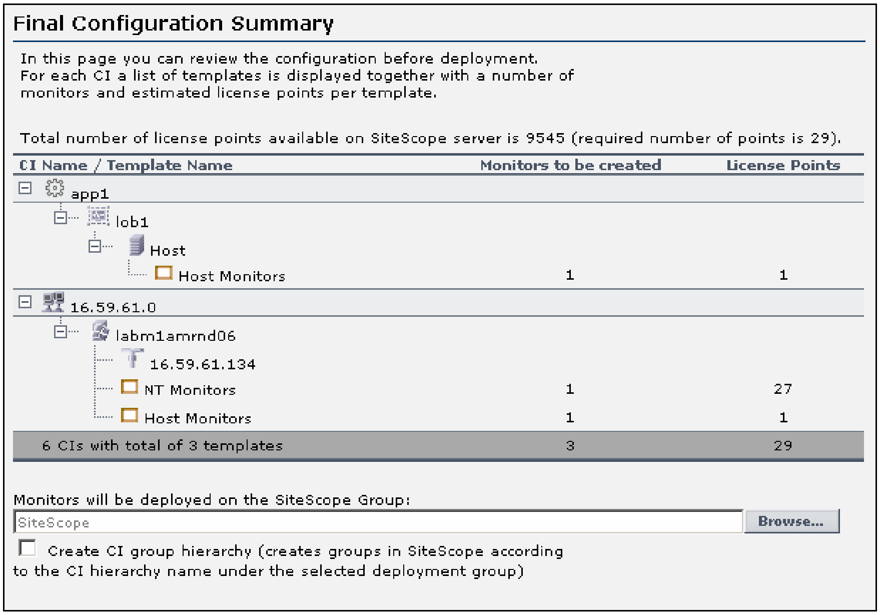
Enter the required data in the fields below to ensure the successful creation of all monitors. All fields must be filled.
Only CIs that lack required data are expanded

CI	Variable	Value
⊟ IT Department		
⊟ ☑ NT Monitors(37 pts)		
	host_dnsname	1.2.3.4
	host_username	user1
	host_password	••••••
	nt_domain	domain1
⊟ 16.59.57.155		
⊟ ☑ Host Monitors(1 pts)		
	Host DNS Name	16.59.57.155
⊟ □ NT Monitors(37 pts)		
	Host DNS Name	16.59.57.155
	host_username	
	host_password	
	nt_domain	

Check the Configuration Summary and Deploy Monitors

On the fourth page of the wizard, review the final configuration summary and select a SiteScope group on which to deploy the templates. Click **Finish** to complete the wizard and deploy the monitors. For details, see “Final Configuration Summary Page” on page 90.

Example:



Final Configuration Summary

In this page you can review the configuration before deployment.
For each CI a list of templates is displayed together with a number of monitors and estimated license points per template.

Total number of license points available on SiteScope server is 9545 (required number of points is 29).

CI Name / Template Name	Monitors to be created	License Points
app1		
lob1		
Host		
Host Monitors	1	1
16.59.61.0		
labm1amrnd06		
16.59.61.134		
NT Monitors	1	27
Host Monitors	1	1
6 CIs with total of 3 templates	3	29

Monitors will be deployed on the SiteScope Group:

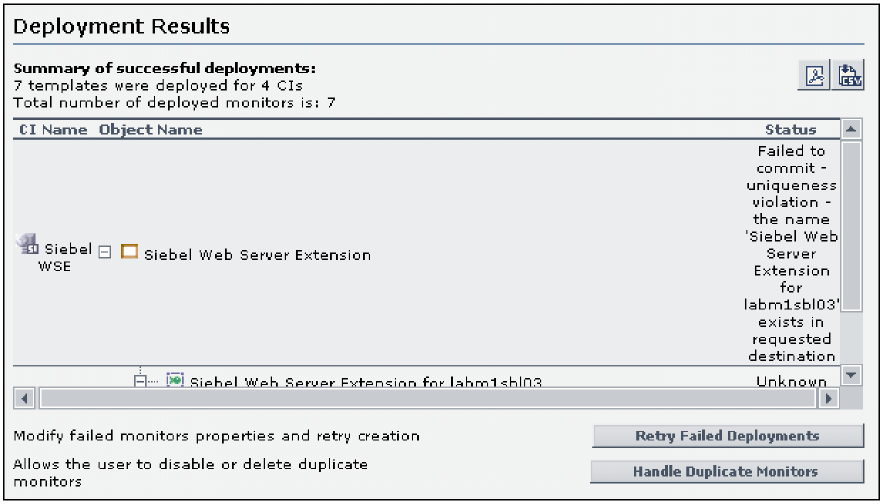
SiteScope

□ Create CI group hierarchy (creates groups in SiteScope according to the CI hierarchy name under the selected deployment group)

Review the Deployment Results and Export the Report

On the last page of the wizard, review the results of the deployment and, if necessary, retry deploying those template that failed to deploy. In this page, you can also handle duplicate monitors that were deployed. Optionally, you can export the deployment results to a .pdf or a .csv file. For details, see “Deployment Results Page” on page 91.

Example:



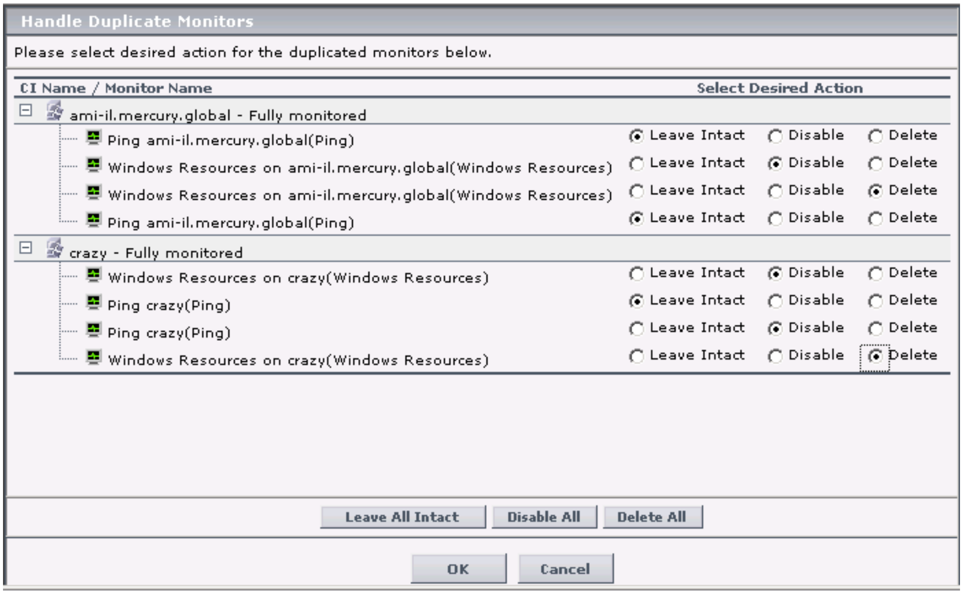
Deployment Results

Summary of successful deployments:
7 templates were deployed for 4 CIs
Total number of deployed monitors is: 7

CI Name	Object Name	Status
Siebel WSE	Siebel Web Server Extension	Failed to commit - uniqueness violation - the name 'Siebel Web Server Extension for labm1sbl03' exists in requested destination
	Siebel Web Server Extension for labm1sbl03	Unknown

Modify failed monitors properties and retry creation

Allows the user to disable or delete duplicate monitors



Handle Duplicate Monitors

Please select desired action for the duplicated monitors below.

CI Name / Monitor Name	Select Desired Action		
⊟ ami-il.mercury.global - Fully monitored			
Ping ami-il.mercury.global(Ping)	● Leave Intact	○ Disable	○ Delete
Windows Resources on ami-il.mercury.global(Windows Resources)	○ Leave Intact	● Disable	○ Delete
Windows Resources on ami-il.mercury.global(Windows Resources)	○ Leave Intact	○ Disable	● Delete
Ping ami-il.mercury.global(Ping)	● Leave Intact	○ Disable	○ Delete
⊟ crazy - Fully monitored			
Windows Resources on crazy(Windows Resources)	○ Leave Intact	● Disable	○ Delete
Ping crazy(Ping)	● Leave Intact	○ Disable	○ Delete
Ping crazy(Ping)	○ Leave Intact	● Disable	○ Delete
Windows Resources on crazy(Windows Resources)	○ Leave Intact	○ Disable	● Delete

Template Reference

The Monitor Deployment Wizard is enabled by a series of templates preconfigured in the SiteScope monitor tree.

Template Reference Table

Following is a table listing all the configuration items onto which the Monitor Deployment Wizard can deploy templates. The table lists the templates and CI types, the monitors which are deployed, the monitor properties imported from the CMDB, and the variable definitions that are either imported from the CMDB or defined within the wizard.

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Apache server	Apache	Apache Server monitor	server name or IP address	application_IP
			application port (default value is 8080)	application_port
IIS server	IIS	IIS Server monitor	server name or IP address	application_IP
			host password	host_password
			user name	host_username
			NT domain	nt_domain
Host	Host	Ping monitor	dns name	host_dnsname
	Windows			
	UNIX			
	Network			
	Switch			
	Router			
	switch-router			

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Windows server	Windows	Windows Resources monitor	dns name	host_dnsname
				host_password
				host_username
				nt_domain
UNIX	UNIX	CPU and Memory monitor, UNIX Remote server		connection_ method
			dns name	host_dnsname
				host_os
				host_password
				host_username
SQL server	sqlserver	SQL Server monitor	server name or IP address	application_IP
				nt_domain
				SqlServerHost Password
				SqlServerHost UserName

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Oracle database	Oracle	Oracle Database monitor	server name or IP address	application_IP
			application password (default value is manager)	application_ password
			application user name (default value is system)	application_user name
			database port (default value is 1521)	database_dbport
			database SID	database_dbsid
UDDI	UDDI Registry	UDDI Server	data_name	data_name
			business_name	business_name
Web Services	Web Service	WSDL	method_name	method_name
				method_ns
			ParamUrl	ParamUrl
				port
			purl	purl
				service_name
			soap_action	soap_action
			WsdlUrl	WsdlUrl

Template Reference for Siebel

Following are tables listing all the Siebel configuration items onto which the Monitor Deployment Wizard can deploy monitors. The Siebel templates are divided according to groups. The table lists the CI Templates and CI types, the monitors which are deployed, the monitor properties imported from the CMDB, and the variable definitions that are either imported from the CMDB or defined within the wizard.

Siebel Application Server Monitor

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Application Server	Application Server	Siebel Application Server log	Server_Name	Server_Name
			Siebel_Root_Dir	Siebel_Root_Dir
			Siebel_Logical_ Instance_Name	Siebel_Logical_ Instance_Name
		Siebel Application Server	Application	Application
			Gateway	Gateway
			Enterprise	Enterprise
			Username	Username
			Server_Manager _Path	Server_Manager_ Path
			PASSWORD	PASSWORD
	Database	Siebel Enterprise Integration Manager process (growth rate)	Database_ Connection_ URL	Database_ Connection_ URL
			Database_Driver	Database_Driver
			Database_ UserName	Database_ UserName
			Database_Server _Name	Database_Server_ Name
			PASSWORD	PASSWORD

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Application Server *cont'd*	Database *cont'd*	Siebel Transaction Logging process (is enabled)	Database_ UserName	Database_ UserName
			Database_Driver	Database_Driver
			Database_ Connection_ URL	Database_ Connection_ URL
			Database_Server _Name	Database_Server_ Name
			Database_PASS WORD	Database_ PASSWORD
		Siebel Transaction Router process (growth rate)	Database_UserN ame	Database_ UserName
			Database_Driver	Database_Driver
			Database_Conn ection_URL	Database_ Connection_URL
			Database_Server _Name	Database_Server_ Name
			Database_PASS WORD	Database_ PASSWORD
		Siebel Workflow Rules process (growth rate)	Database_UserN ame	Database_ UserName
			Database_Driver	Database_Driver
			Database_Conn ection_URL	Database_ Connection_URL
			Database_Server _Name	Database_Server_ Name
			Database_PASS WORD	Database_ PASSWORD

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Application Server Host	Host	Disk Space	Server_Name	Server_Name
		Ping	Server_Name	Server_Name
		Memory	Server_Name	Server_Name
		CPU Utilization	Server_Name	Server_Name
		Directory log	Server_Name	Server_Name
			Siebel_Root_Dir	Siebel_Root_Dir
		Service Siebel Server	Server_Name	Server_Name
			Enterprise	Enterprise
			Server_Logical_ Instance_Name	Server_Logical_ Instance_Name
		Directory	Server_Name	Server_Name
			Siebel_Root_Dir	Siebel_Root_Dir
Siebel Component	Siebel Component	Siebel Component log	alias	alias
			Server_Name	Server_Name
			Application	Application
			Siebel_Root_ Dir	Siebel_Root_ Dir
			Siebel_Logical_ Instance_Name	Siebel_Logical_ Instance_Name
		Siebel Component	alias	alias
			Username	Username
			Enterprise	Enterprise
			Application	Application
			Gateway	Gateway
			Server_Manager _Path	Server_Manager_ Path
			Server_Logical_ Instance_Name	Server_Logical_ Instance_Name
			PASSWORD	PASSWORD
			Group_Name	Group_Name
			data_name	data_name

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Component Group	Siebel Component Group	Siebel Component Group on	alias	alias
			Server_Logical_ Instance_Name	Server_Logical_ Instance_Name
			Enterprise	Enterprise
			Application	Application
			Gateway	Gateway
			data_name	data_name
			Server_Manager _Path	Server_Manager_ Path
			Server_Name	Server_Name
			PASSWORD	PASSWORD

Siebel Gateway Monitors

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Gateway Server Host	Host	CPU Utilization	Server_Name	Server_Name
		Directory	Server_Name	Server_Name
			Siebel_Root_Dir	Siebel_Root_Dir
		Disk Space	Server_Name	Server_Name
		Memory	Server_Name	Server_Name
		Ping	Server_Name	Server_Name
		Service	Server_Name	Server_Name

Siebel Web Server Monitors

Template	CI Type	Applicable Monitor	Discovered Properties	Variables
Siebel Web Server Extension	Siebel Web Server Extension	Service	Server_Name	Server_Name
		Siebel Web Server	Server_Name	Server_Name
			Application	Application
			Username	Username
			PASSWORD	PASSWORD
		URL	Server_Name	Server_Name
			Application	Application
			Username	Username
			PASSWORD	PASSWORD
Siebel Web Server Host	Host	CPU Utilization	host_dnsname	host_dnsname
		Directory	host_dnsname	host_dnsname
			Siebel_Root_Dir	Siebel_Root_Dir
		Disk Space	host_dnsname	host_dnsname
		Memory	host_dnsname	host_dnsname
		Ping	host_dnsname	host_dnsname
		Service	host_dnsname	host_dnsname
Web Server	Web Server	IIS Server	host_dnsname	host_dnsname
		Port 80	host_dnsname	host_dnsname

4

Monitor Deployment Wizard User Interface

This chapter includes a description of the pages and dialog boxes that are part of the Monitor Deployment Wizard user interface.

Note: The Monitor Deployment Wizard is available only to those users accessing SiteScope from System Availability Management Administration in HP Business Availability Center.

Monitor Deployment Wizard

Description	Enables you to deploy SiteScope monitors using the configuration item data from the CMDB using pre-defined templates. **To access:** Select **Admin** > **System Availability Management.** Right-click the appropriate SiteScope server or group and select **Monitor Deployment Wizard** or click the **Monitor Deployment Wizard** icon in the Summary page next to the appropriate SiteScope server.
Important Information	The wizard is accessible only if you have a running SiteScope hosted in System Availability Management Administration. After running the Monitor Deployment Wizard, the deployed monitors do not begin to run immediately, but rather within the defined monitor running frequency time. You must give the system time to implement all the updates.
Included in Tasks	"Deploy Monitors Using the Monitor Deployment Wizard" on page 68
Useful Links	"Monitor Deployment Wizard Concepts and Tasks" on page 59
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

Welcome Page

Description	Enables you to synchronize the SiteScope adapter to update all monitor data.
Important Information	An error message appears when you attempt to proceed to the next page if: ➤ the SiteScope you selected is not available or ➤ the CMDB is not available For general information about the Monitor Deployment Wizard, see "Monitor Deployment Wizard" on page 84.
Useful Links	"Work with the SiteScope Source Adapter" in *IT World Model Management*.
Wizard Map	The Monitor Deployment Wizard contains: **Welcome Page** > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

The Welcome page includes the following element:

GUI Element	Description
Synchronize the latest SiteScope configuration	Select to synchronize the SiteScope adapter to update all monitor data. This may take up to 30 minutes depending on how many SiteScope monitors are deployed in your environment and when the last synchronization took place. Synchronization occurs automatically on an hourly basis, so if you are running the wizard just after a scheduled synchronization, it is unnecessary to select the check box.

Select CIs to Monitor Page

Description	Enables you to select CIs onto which to deploy the SiteScope monitors.
Important Information	If a CI appears under more than one view in the left pane, you cannot select it more than once in the selection that appears in the right pane, even if you attempt to select it from different views. The wizard checks for full and partial monitor coverage of the selected CIs. You have the option of deploying the template onto these CIs and handling duplicate monitors.
Useful Links	"Monitor Deployment Wizard Templates and Variables" on page 63 "Full and Partial Monitor Coverage" on page 65
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > **Select CIs to Monitor Page** > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

The Select CIs to Monitor page includes the following element:

GUI Element	Description
<View Explorer>	The Select CIs to Monitor page uses the standard View Explorer functionality to select CIs in the left pane and move them to the right pane. For details, see “View Explorer User Interface” in *Reference Information*. **Note:** The wizard cannot create monitors for the following CIs: ➤ CIs that do not have a matching template for deploying a monitor type ➤ CIs that are monitor CIs, generally those appearing in the monitor view If you selected any CIs of these types, a warning message appears when you attempt to proceed to the next step of the wizard.

Templates Selection Dialog Box

Description	Enables you to apply templates to CI Types which were not automatically matched by the wizard. **To access:** Click the **Templates Selection** button from the Select CI to Monitor step of the Monitor Deployment Wizard.
Important Information	The Monitor Deployment Wizard automatically matches templates to the CI Types of the selected CIs. You can add additional templates manually in this dialog box. To select multiple templates to add, use the CTRL key. The selected templates are added to all of the selected CI Types.

Useful Links	"Monitor Deployment Wizard Templates and Variables" on page 63
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > **(Templates Selection Dialog Box)** > Enter Required Data for CIs Page > Final Configuration Summary Page > Deployment Results Page

The Templates Selection dialog box includes the following elements:

GUI Element	Description
➡	Click to add the selected templates in the left pane to the CI selection in the right pane.
⬅	Click to remove selected templates from the CI selection.
<Template list>	The left pane lists all the available templates in the wizard. The child objects are the monitors that are deployed by the template.
<CI Type Selection>	The right pane lists the CI Types of all the CIs selected in the Select CI to Monitor step of the Monitor Deployment Wizard. If the wizard was able to match templates to the selected CI Types, the CI Type is listed with the applicable template as a child object.
Save Matching	Select the check box to save your template selection as a preference. This includes those templates that are selected manual for CI types and those that are cleared from the automatic selection of the wizard. The manually adjusted templates selection is matched to the selected CIs automatically the next time the same Business Availability Center user runs the wizard.
Restore Defaults	Click to reset the list and remove all the added templates from the CI Types (the ones added automatically by the wizard remain).

Enter Required Data for CIs Page

Description	Enables you to fine tune your template selection for specific CIs and fill in the missing information for those templates.
Important Information	If data is missing for any selected templates, an error appears and you are unable to proceed to the next step. If any templates are unselected, a warning appears before you proceed to the next step that informs you that there are unselected templates. This applies whether data is filled in for the unselected templates or not.
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > **Enter Required Data for CIs Page** > Final Configuration Summary Page > Deployment Results Page

The Enter Required Data for CIs page includes the following elements:

GUI Element	Description
<Expanded CI list>	The CIs that are missing required data are expanded. (If no CIs are missing data, this section does not appear.)
<Unexpanded CI list>	CIs that are not missing data are not expanded. You can optionally expand the CIs to modify the data. (If all CIs are missing data, this section does not appear.)
CI column	Each template for each CI is displayed separately with the relevant number of license points for that template. Select the check box for the CI and template combinations for which you want to deploy monitors.
Variable column	The variables for templates with missing data are listed in the Variable column.
Value column	Enter the missing data in the Value column for all the selected templates. You can tab between the fields and enter the required data in the available fields. (You do not need to enter missing data for templates that are not selected.)

Final Configuration Summary Page

Description	Displays a list of the monitors about to be deployed and enables you to select the SiteScope group onto which they are deployed.
Important Information	Above the table, a note displays the total number of license points available on the SiteScope server (after the current action is complete). If the number of license points required for the current action exceeds your available points, a warning appears to tell you to remove some of the selected templates.
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > **Final Configuration Summary Page** > Deployment Results Page

The Final Configuration Summary page includes the following elements:

GUI Element	Description
CI Name/Template Name column	Lists each selected CI with its templates.
Monitors to be Created column	Indicates the number of monitors being created for each template.
License Points column	Indicates the number of SiteScope license points required for each monitor.

GUI Element	Description
SiteScope Group selection window	To select the SiteScope group under which the monitors are deployed, click **Browse** and select a group from the tree in the Choose Target SiteScope Group dialog box. **Note:** If you attempt to deploy the same monitor on the same CI in the same group twice, the deployment fails with a unique name error. However, you may select a different group under which to deploy that monitor onto that CI.
Create CI group hierarchy	Select the check box to create a CI group hierarchy. This creates SiteScope groups under the target group with the identical hierarchy of the CIs. For details, see "CI Group Hierarchy Option" on page 66.

Deployment Results Page

Description	Displays a summary of the successful and unsuccessful template deployments.
Important Information	The deployment of monitors occurs at the template level. This means that if the deployment fails for any of the template elements (monitor, group, remote, or alert), no other monitors in the template are deployed. When you deploy a physical monitor (for example, a CPU monitor), a remote server with the same name is also created if such a remote server does not already exist under Remote Preferences (Windows or UNIX).
Wizard Map	The Monitor Deployment Wizard contains: Welcome Page > Select CIs to Monitor Page > (Templates Selection Dialog Box) > Enter Required Data for CIs Page > Final Configuration Summary Page > **Deployment Results Page**

The Deployment Results page includes the following elements:

GUI Element	Description
	Click to export the Monitor Deployment Wizard Summary page to a PDF. This report includes all created entities in SiteScope displaying the deployment directory and status. It also displays the status of duplicate monitors.
CSV	Click to export the Monitor Deployment Wizard Summary page to a CSV file. This report includes all created entities in SiteScope displaying the deployment directory and status. It also displays the status of duplicate monitors.
CI Name column	Lists the names of the selected CIs.
Object Name column	Lists the monitors selected for deployment onto a given CI.
Status column	Indicates whether the deployment succeeded or not.
Retry Failed Deployments	Click **Retry Failed Deployments** to re-attempt to deploy those monitors whose deployment failed by modifying the data entered in the Enter Required Data for CIs page. **Note:** This button appears only if there were failed deployments.
Handle Duplicate Monitors	If duplicate monitors were deployed, click **Handle Duplicate Monitors** to open the Handle Duplicate Monitors dialog box. For each duplicate monitor listed, you can select to leave it intact, disable it, or delete it. If all the monitors are to be handled in the same way, you can use the **Leave All Intact**, **Disable All** or **Delete All** buttons at the bottom of the page. For details on understanding duplicate monitors, see "Full and Partial Monitor Coverage" on page 65.

5

Introduction to System Availability Management Reports

HP System Availability Management reports enable you to monitor system availability data across the entire enterprise.

Note: The System Availability Management reports are available only to HP Business Availability Center users.

Overview of System Availability Management Reports

You use the System Availability Management application to view and analyze reports based on the performance data collected by the SiteScope data collector and stored in the HP Business Availability Center database.

In addition, using SiteScope Infrastructure Monitors, you can integrate data collected by enterprise management systems (such as BMC Patrol, Tivoli, Concord, and NetIQ) into HP Business Availability Center, and view the data in System Availability Management reports.

System Availability Management utilizes data collected by SiteScope and enables you to:

- monitor system availability across the entire enterprise infrastructure from a centralized, real-time perspective
- apply a business perspective to system management
- view data at the application level rather than viewing numerous low-level system metrics
- view information about events collected from external applications or software and SiteScope events

Note:

- You access the System Availability Management reports from the System Availability Management application in the Applications menu.
- For details on working with HP Business Availability Center reports, see "Working in Reports" in *Reference Information*.

This section includes the following topics:

- "Report Access and Permissions" on page 94
- "Data Aggregation" on page 95
- "List of Available System Availability Management Reports" on page 95

Report Access and Permissions

The availability of report data to a specific user is dependent on the profile access permissions granted that user. Furthermore, access to specific data within a profile may also be filtered by using the group permission filters. For details on granting permissions, see "Permissions Management" in *Platform Administration*. For details on defining group permission filters, see "Set Group Permissions for Reports" on page 126.

Data Aggregation

HP Business Availability Center uses data aggregation to make data handling and management more efficient and to improve the speed and performance of report generation. For more information on data aggregation in HP Business Availability Center, see “Data Aggregation” in *Reference Information*.

List of Available System Availability Management Reports

The following reports are available:

Tab Name	Description	For Details, See...
SiteScope Over Time Reports	View and analyze reports, based on data collected by SiteScope, that help you track the performance of your infrastructure machines and provide insight into application availability and performance.	“SiteScope Over Time Reports” on page 99
Event Log	View event data over time, events that happened at a specific time, the details of a specific event, and event history.	“The Event Log” on page 131
User Reports	Provides tools for creating, and displays, reports that are tailored to the specific monitoring requirements of your organization or business unit. Report data is based on Business Process Monitor, WebTrace/Traceroute Monitor, SiteScope, and Custom data.	“User Reports” on page 143

Working with System Availability Management Reports

System Availability Management reports help you identify server resource usage trends, as well as bottlenecks and other server-related issues that may be contributing to application performance problems. You can continually monitor report data to identify poor server performance or to spot developing trends that may lead to server performance problems.

Alternatively, when you become aware of an application performance problem with your application (for example, after analyzing End User Management reports or receiving an alert), you can use System Availability Management reports to help you identify, or rule out, infrastructure machine-related issues as the root cause of the problem. By analyzing the infrastructure machine resource usage data for the same time period during which the performance problem occurred, you can assess whether one or more infrastructure machine resource measurements are outside normal performance thresholds for that time period.

This section includes the following topics:

- "Color Coding in Reports" on page 96
- "Improving Report Generation Times" on page 97

Color Coding in Reports

System Availability Management reports use the following colors when displaying color-coded performance levels:

Color	Description
Green	All measurements fell within the OK threshold range.
Yellow	At least one measurement fell within the minor threshold range, but no measurements fell within the critical threshold range.
Red	At least one measurement fell within the critical threshold range.
Gray	No measurement data reported.

Improving Report Generation Times

Note to HP Managed Software Solutions customers: This section is not relevant for HP Managed Software Solutions customers.

To optimize the performance of System Availability Management report generation, we recommend that a database administrator perform an update statistics procedure on the database on a regular basis. The regularity of the update depends on the amount of data generated by the applications you are monitoring.

- **MS SQL Server users:**
  - for a small site, you should update once every three to four days
  - for a medium site, you should update daily
  - for a large site, you should update every four hours

    For details on MS SQL Server maintenance, see "Maintenance Plan" in the *HP Business Availability Center Database Guide* PDF.
- **Oracle Server users.** Analyze all tables according to database size.

  For details on optimizing performance in Oracle, see "Collecting Statistics for Databases" in the *HP Business Availability Center Database Guide* PDF.

6

SiteScope Over Time Reports

This chapter describes SiteScope Over Time reports which are based on data collected by the SiteScope data collector.

Note: The System Availability Management reports are available only to HP Business Availability Center users.

Understanding SiteScope Over Time Reports

You use the SiteScope Over Time reports to view and analyze infrastructure machine-related data collected by the SiteScope data collector and stored in the HP Business Availability Center database. You cross-reference this data with transaction performance problems, such as slow transaction response times and failed transactions, to understand the root cause of application performance issues.

The contents of SiteScope Over Time reports depend on the types of SiteScope monitors and measurements that are defined in System Availability Management Administration.

HP Business Availability Center users can use group permissions filters to control the data that System Availability Management reports display. This enables filtering data that may be irrelevant to a specific user, making reports more manageable and report generation faster. For details, see "Set Group Permissions for Reports" on page 126.

Note:

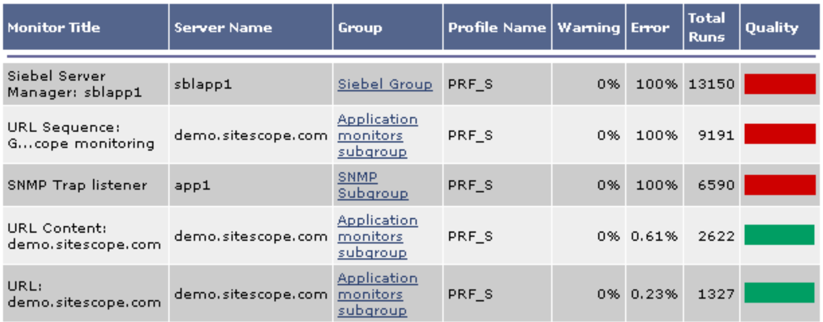
- For details on generating reports, see "Working in Reports" in *Reference Information*.
- Certain System Availability Management reports can be added to custom reports. For details, see "System Availability Management Data in Custom Reports" on page 129.
- Data collected by the SiteScope data collector can also be viewed in trend reports. Trend reports enable you to compare multiple measurements from different data sources on the same graph. For details, see "Trend Report Manager" in *Custom Reporting and Alerting*.
- If a SiteScope contains many measurements, report generation can take a few minutes.

The following System Availability Management reports are available:

Report	**Description**	**For Details, See...**
Monitor Performance Report	Displays the best- or worst-performing SiteScope monitors across various SiteScope categories.	page 102
Cross-Performance Report	Displays data from more than one SiteScope server filtered by monitored servers, monitor types, and measurements.	page 105
Group Performance Report	Displays the infrastructure machine resource usage data for the monitors in the selected group and its subgroups.	page 118
Status Summary Report	Displays a quick snapshot of the performance of monitored infrastructure machines, organized by SiteScope group.	page 122
Warning Summary Report	Displays a list of the monitors, for the selected group and its subgroups, whose measurements fell within the minor threshold level during the selected time period.	page 123
Error Summary Report	Displays a list of the monitors, for the selected group and its subgroups, whose measurements fell within the critical threshold level during the selected time period.	page 125
Set Group Permissions for Reports	Enables you to filter data for specific SiteScope groups or subgroups from System Availability Management reports, as well as the SiteScope Monitor Performance component in custom reports.	page 126

Monitor Performance Report

You generate the Monitor Performance report to view the best- or worst-performing SiteScope monitors across various SiteScope categories, such as monitor type, monitored server, or monitor title. You can generate a Monitor Performance report for multiple SiteScope profiles.



Monitor Title	Server Name	Group	Profile Name	Warning	Error	Total Runs	Quality
Siebel Server Manager: sblapp1	sblapp1	Siebel Group	PRF_S	0%	100%	13150	🟥
URL Sequence: G...cope monitoring	demo.sitescope.com	Application monitors subgroup	PRF_S	0%	100%	9191	🟥
SNMP Trap listener	app1	SNMP Subgroup	PRF_S	0%	100%	6590	🟥
URL Content: demo.sitescope.com	demo.sitescope.com	Application monitors subgroup	PRF_S	0%	0.61%	2622	🟩
URL: demo.sitescope.com	demo.sitescope.com	Application monitors subgroup	PRF_S	0%	0.23%	1327	🟩

This section includes the following topics:

- "Generate the Monitor Performance Report" on page 102
- "Understanding the Monitor Performance Report" on page 103

Generate the Monitor Performance Report

To view the Monitor Performance report, you specify the criteria upon which you want the report to be based and generate the report.

To generate the Monitor Performance report:

1. Access the Monitor Performance report: **Applications** > **System Availability Management** > **SiteScope Over Time Reports** > **Monitor Performance**.
2. Select the SiteScope for which you want to view the report.

3 In the **Monitor title** and **Server name** boxes, specify the monitors (by their title, as defined in SiteScope) and/or servers on which you want the custom report data to be based.

Leave a box empty to instruct HP Business Availability Center to base the report on all values.

If required, you can use the wildcard asterisk symbol (*) to instruct HP Business Availability Center to base the report on a subset of all values. For example, if you are using the naming convention cpu_<servername> to name all CPU monitors in SiteScope, specify cpu* to instruct HP Business Availability Center to include all CPU monitors in the custom report.

Note: Using the wildcard asterisk symbol (*) as the first character in the string slows report generation times, as HP Business Availability Center is unable to use the Index tables when querying the database.

4 From the **Monitor type** list, select the monitor on which you want the report data to be based. To base the report on all monitors, choose **All types**.

5 Specify whether you want HP Business Availability Center to display the worst- or best-performing monitors, and choose the number of monitors to be displayed in the report.

6 Click **Generate** to generate the report.

Understanding the Monitor Performance Report

The Monitor Performance report displays the following information:

- **Monitor Title.** The monitor title. Hold the pointer over the tooltip to view the full monitor title.
- **Server Name.** The name of the monitored server. Hold the pointer over the tooltip to view the full server name.
- **Group.** The group or subgroup in which the monitor is defined. Hold the pointer over the tooltip to view the path from the displayed group or subgroup to the root group. Click the group or subgroup name to open the management page for the group in SiteScope.

- **Profile Name.** The name of the SiteScope profile in which the monitor is defined.
- **Warning.** The percentage of measurement instances that return a critical-level threshold status.
- **Error.** The percentage of measurement instances that return an error-level threshold status.
- **Total Runs.** The total number of measurement instances SiteScope ran for the selected time range.
- **Quality.** A color-coded representation of quality. Hold the pointer over the tooltip to view the exact percentage for each colored section of the bar.

  Monitors are sorted in the report by quality, which is derived using a formula that takes into account the measurement values returned for the monitor during the specified time range relative to the measurement threshold ranges configured in SiteScope.

  The formula used is: **1-((0.35*W+0.5*E)/(G+W+E))**, where G, W, and E represent the number of measurements that occurred during the selected time range whose value was within the OK, Warning, and Error threshold range, respectively. The formula returns values from 0.5 to 1, inclusively. The better a monitor performs, the closer its value is to 1. For example, a monitor with 25% error and 75% OK values would be displayed as better than a monitor with 100% Warning values.

Note: The Monitor Performance report does not use raw data. All data in the report is based on aggregated data.

Cross-Performance Report

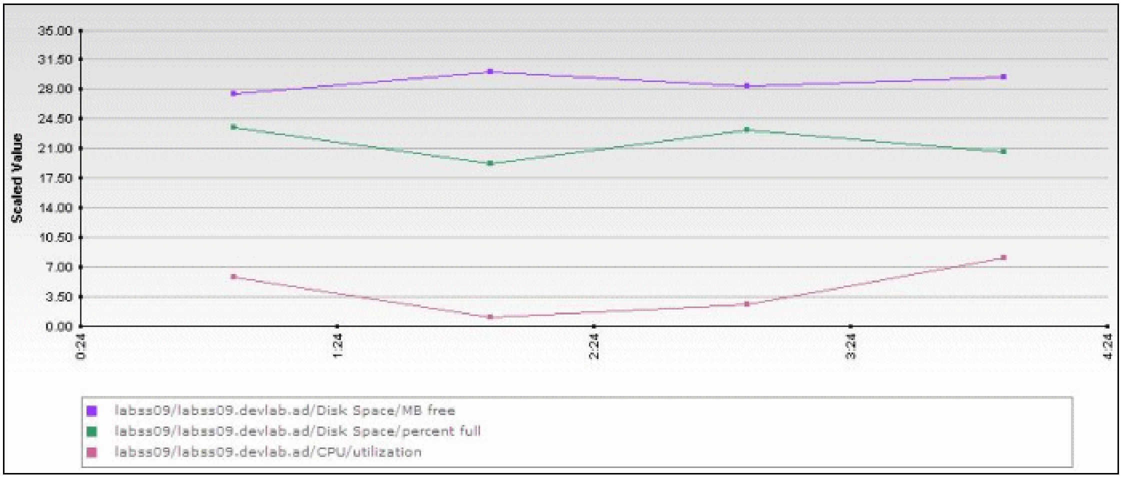
The Cross-Performance reports can be displayed in the following formats:

- **Graph per measurement.** For details, see “Graph Per Measurement” on page 112.
- **One graph for all measurements.** For details, see “One Graph for All Measurements” on page 113.
- **Table view.** For details, see “Table View” on page 114.

You can rescale a SiteScope cross-performance report to make it more relevant to what you are measuring. For details, see “Rescaling a Cross-Performance Report” on page 115.

You can view data from more than one SiteScope. You can filter the data by monitored servers, monitor type or title, and measurements.

For example, you can display the behavior of a measurement running on several monitored servers, or the behavior of several measurements from various types of monitors running on one monitored server.



Note: If you are running a SiteScope Log File or Database Query monitor that is monitoring a different machine, you should select the SiteScope machine running the monitors in the Servers list, and not the monitored machine (the target machine where the log file or database is located).

You can rescale the report to make it more relevant to what you are measuring.

This section includes the following topics:

Generate a SiteScope Cross-Performance Report

To view the SiteScope Cross-Performance report, specify the time period and granularity, the filters, the type of report, and generate the report.

To generate the SiteScope Cross-Performance report:

1. Access the SiteScope Cross-Performance report: **Applications** > **System Availability Management** > **SiteScope Over Time Reports** > **SiteScope Cross-Performance**.
2. Select the time period and the granularity with which you want to run the report. For details, see "Choosing the Time Range and Granularity" in *Custom Reporting and Alerting*.

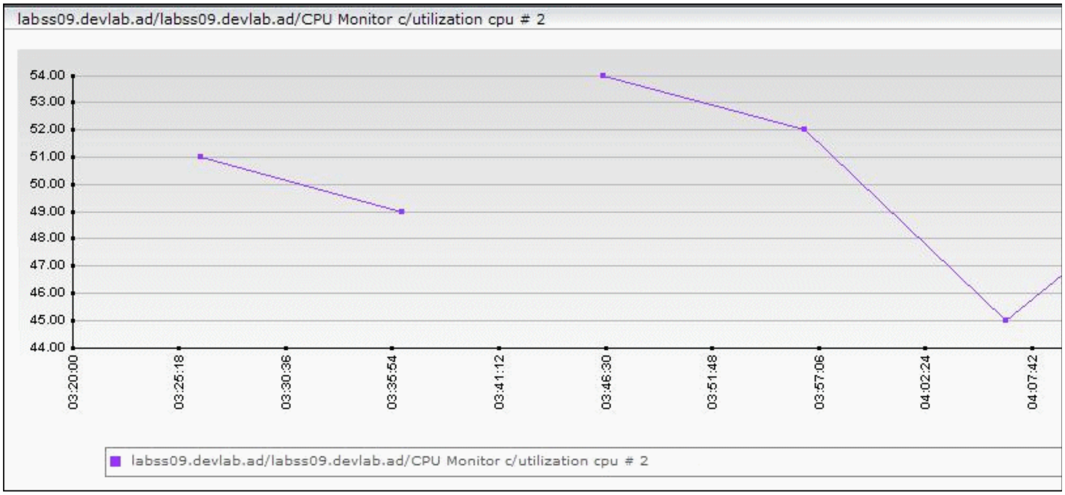
   The granularity determines how many measurement samples are displayed in the report for each time interval. By default, the number of samples is limited to the maximum value of the **Max Data Points in Report** setting (32 by default for all reports where you can specify the granularity).

   Note: You can change these settings in the Infrastructure Settings Manager. To modify these settings, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **End User/System Availability Management** and locate **Max Data Points in Report** in the **End User/System Availability Management - Data** table. For details on using the Infrastructure Settings Manager, see "Infrastructure Settings" in *Platform Administration*.

   You can choose to view raw data on the given report by selecting the **Raw Data** option on the time period and granularity bar. There are several factors to keep in mind when choosing this option:

➤ A point on the graph appears when there is a change in the data value or measurement frequency from the previous time point on the graph. However, if there has been no change in either of these areas over the course of one hour, a point is nevertheless displayed on the graph.

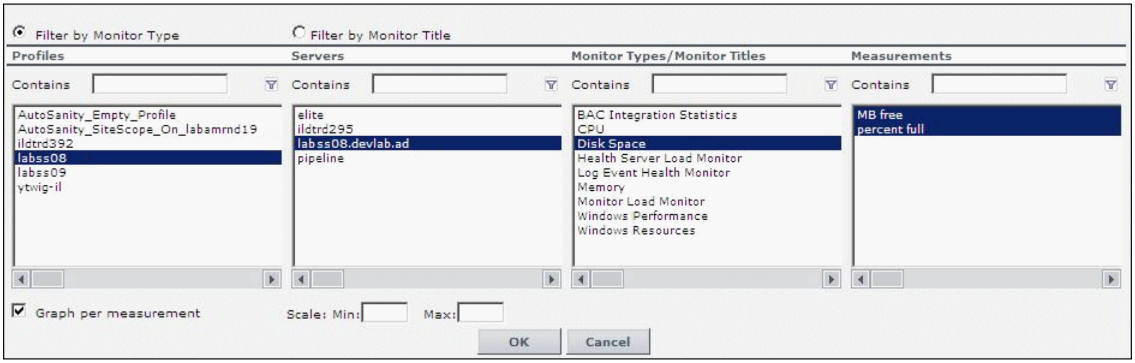
- A straight line on the graph with no points indicates the following:
  - There has been no change in the value of the incoming data from the previous time point on the graph.
  - There has been no change in the frequency that the incoming data is measured in since the previous time point on the graph.
- A gap in the graph indicates that no data has been retrieved for the specific time period.



3 Choose whether to display the monitor type or title when selecting the component to add to the report:

- **Monitor type.** The type of monitor is displayed, for example, Ping, CPU.
- **Monitor title.** The name given to the specific monitor is displayed, for example, ping: myserver, CPU finance_server.

4 Filter the data you want to include in the report:



● Filter by Monitor Type ○ Filter by Monitor Title

Profiles — Contains:
- AutoSanity_Empty_Profile
- AutoSanity_SiteScope_On_labamrnd19
- ildtrd392
- labss08
- labss09
- ytwig-il

Servers — Contains:
- elite
- ildtrd295
- labss08.devlab.ad
- pipeline

Monitor Types/Monitor Titles — Contains:
- BAC Integration Statistics
- CPU
- Disk Space
- Health Server Load Monitor
- Log Event Health Monitor
- Memory
- Monitor Load Monitor
- Windows Performance
- Windows Resources

Measurements — Contains:
- MB free
- percent full

☑ Graph per measurement Scale: Min: Max:

➤ From the **Profile** list (sorted alphabetically), select one or more SiteScope profiles.

➤ From the **Server** list, select one or more servers. The list includes all monitored servers associated with the selected profiles, in alphabetical order.

➤ Depending on whether you chose **Filter by Monitor Type** or **Filter by Monitor**, the **Monitor Types/Monitor Titles** list displays monitor types or monitor names, associated with the selected profiles and servers, in alphabetical order. Select one or more monitors.

➤ From the **Measurements** list, select one or more measurements. The list includes the measurements that are associated with the selected profiles, servers, and monitor types, in alphabetical order.

If you select a measurement for which data exists from more than one group or profile for the same target server, the data is averaged together in the report. For example, if you have two SiteScope profiles each containing two groups, and in three of those groups the Ping monitor is set up to monitor the same server, if you select both profiles and the round trip time measurement, all round trip time data collected from all three groups in both profiles is displayed in the report as an average value.

Note: To list all the elements whose name includes the string, enter a string in one of the **Contains** boxes and click the filter button.

5. To consolidate data per measurement, select **Graph per measurement**. For details, see “Graph Per Measurement” on page 112 and “One Graph for All Measurements” on page 113. This option is selected by default.
6. If required, enter scale information in the **Scale Min** and **Max** boxes. For details, see “Rescaling a Cross-Performance Report” on page 115.
7. Click **Generate** to generate the report. The filter area of the page closes and the report is displayed.
8. You can print the report, send it by e-mail, or open it in CSV or PDF format. For details, see “Sharing and Storing Reports” in *Custom Reporting and Alerting*.

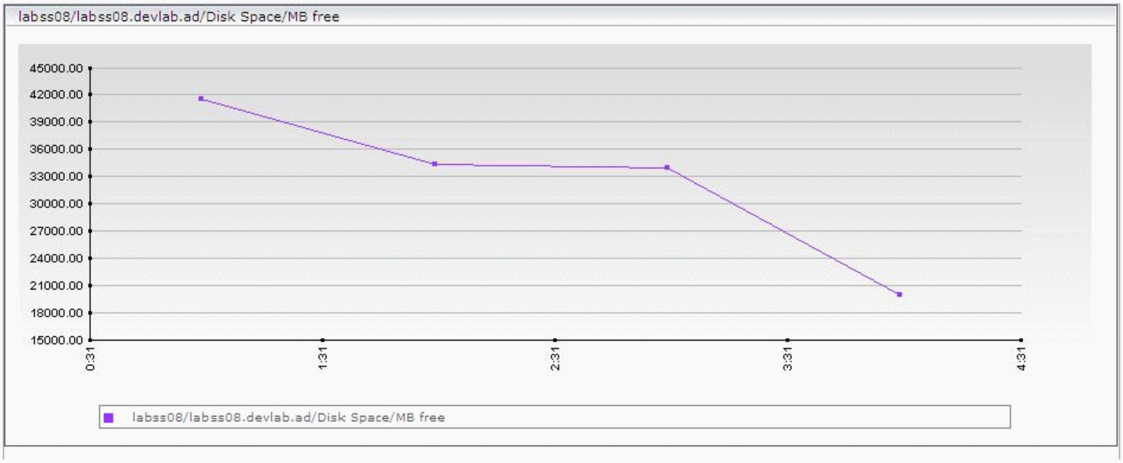
Note:

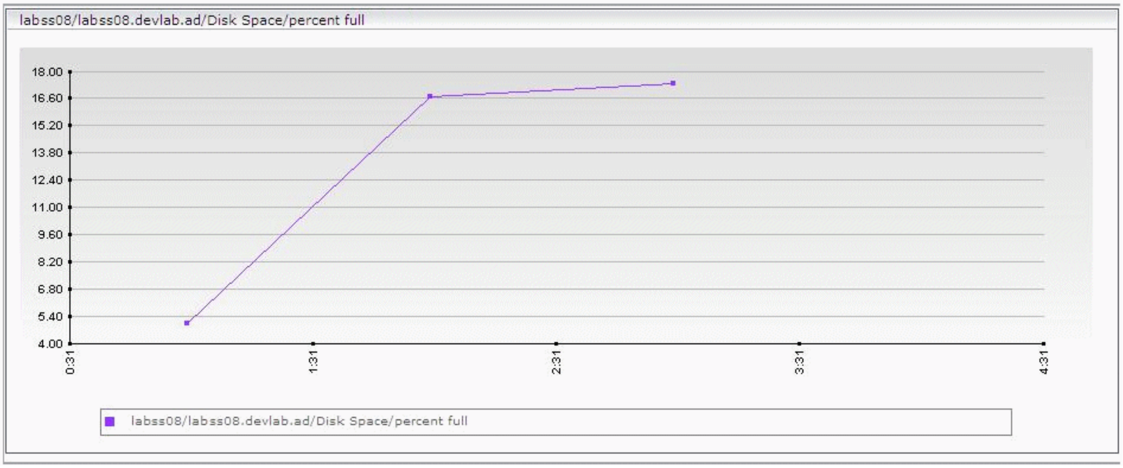
- You cannot generate a report if you have not selected at least one measurement.
- In certain reports the selected time range is displayed along the x-axis. System Availability Management breaks down the time range according to segments, which differ depending on the selected time range. For details on how System Availability Management breaks down each time range in reports where time is displayed along the x-axis, see “Report Times” in *Reference Information*.
- Depending on the time range you select, System Availability Management generates reports using either raw data or aggregated data. The text: **Note: Report uses aggregated data** is displayed in the report when aggregated data is used. For details on how System Availability Management determines when to use aggregated data, see “Data Aggregation” in *Reference Information*.
- The number of selected profiles are calculated after you click **Generate**. You can choose up to 10 profiles. If these numbers exceed the allowed limit, a message is displayed.

Graph Per Measurement

If you select the **Graph per measurement** box, System Availability Management displays each measurement in a separate graph. The graph legend displays the server on which the measurement is running.

The graph legend displays information about the servers. The x-axis displays date and time information and the y-axis displays the measurement value and the monitor type. For example, the following graph displays two measurements running on the labss08 server.



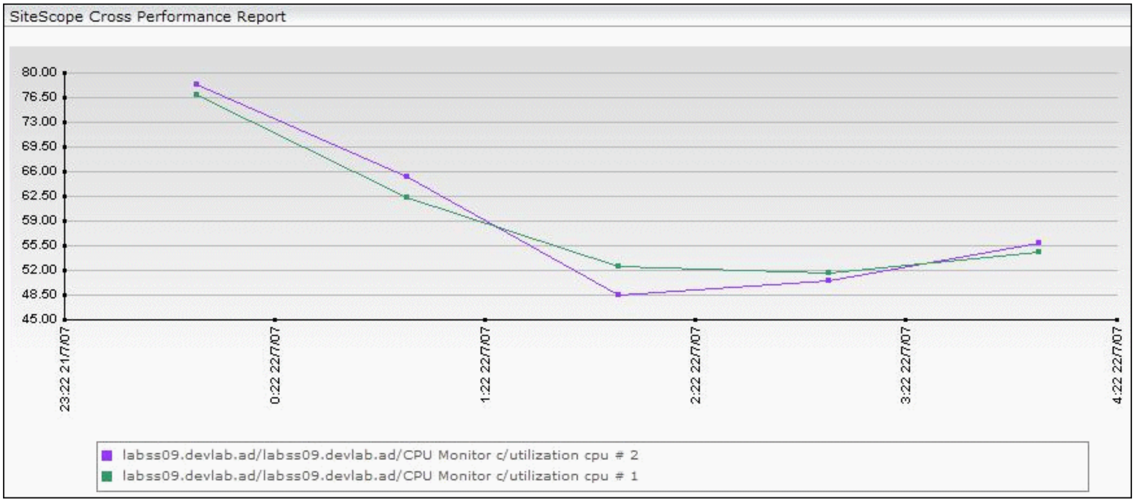


One Graph for All Measurements

If you clear the **Graph per measurement** box, System Availability Management displays one graph for all measurements.

The graph legend displays the measurement value and the monitor type. The x-axis displays the date and time information, and the y-axis shows the measurement values.

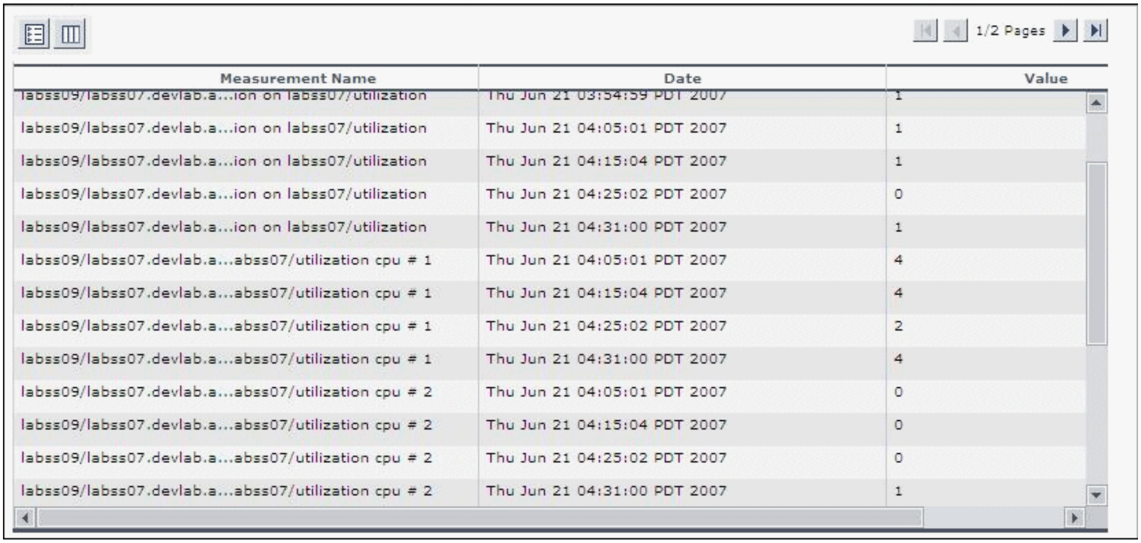
For example, the following graph displays three measurements running on one of the servers.



Each graph displays data for a given measurement. A new graph is created for each different measurement with the title <**server_name**> **continued**.

Table View

If you select **View as table**, the report displays the data in table format. Each table displays the measurement name (including the servers on which the measurement is running, the data and time of the measurement, and the value of the measurement. Click on the column header of the column you want to sort the table by, either in ascending or descending order.



Measurement Name	Date	Value
labss09/labss07.devlab.a...ion on labss07/utilization	Thu Jun 21 03:54:59 PDT 2007	1
labss09/labss07.devlab.a...ion on labss07/utilization	Thu Jun 21 04:05:01 PDT 2007	1
labss09/labss07.devlab.a...ion on labss07/utilization	Thu Jun 21 04:15:04 PDT 2007	1
labss09/labss07.devlab.a...ion on labss07/utilization	Thu Jun 21 04:25:02 PDT 2007	0
labss09/labss07.devlab.a...ion on labss07/utilization	Thu Jun 21 04:31:00 PDT 2007	1
labss09/labss07.devlab.a...abss07/utilization cpu # 1	Thu Jun 21 04:05:01 PDT 2007	4
labss09/labss07.devlab.a...abss07/utilization cpu # 1	Thu Jun 21 04:15:04 PDT 2007	4
labss09/labss07.devlab.a...abss07/utilization cpu # 1	Thu Jun 21 04:25:02 PDT 2007	2
labss09/labss07.devlab.a...abss07/utilization cpu # 1	Thu Jun 21 04:31:00 PDT 2007	4
labss09/labss07.devlab.a...abss07/utilization cpu # 2	Thu Jun 21 04:05:01 PDT 2007	0
labss09/labss07.devlab.a...abss07/utilization cpu # 2	Thu Jun 21 04:15:04 PDT 2007	0
labss09/labss07.devlab.a...abss07/utilization cpu # 2	Thu Jun 21 04:25:02 PDT 2007	0
labss09/labss07.devlab.a...abss07/utilization cpu # 2	Thu Jun 21 04:31:00 PDT 2007	1

Tables display the following information:

- **Measurement Name.** The name of the measurement, including the server on which it is running.
- **Date.** The date and time of the measurement.
- **Value.** The value of the specific measurement.

Rescaling a Cross-Performance Report

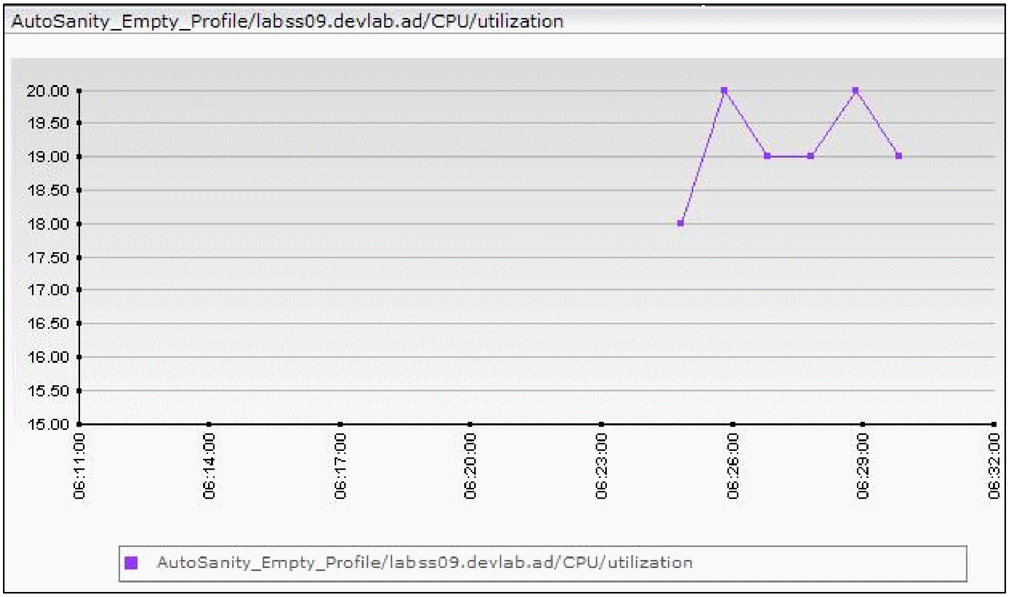
Cross-performance reports are generally scaled so that the lowest y-axis value is zero and the highest y-axis value is the highest result of the data.

You can rescale the report to make it more relevant to the measurement. For example, to measure CPU utilization, you can rescale the report so that the y-axis range is 0 to 100.

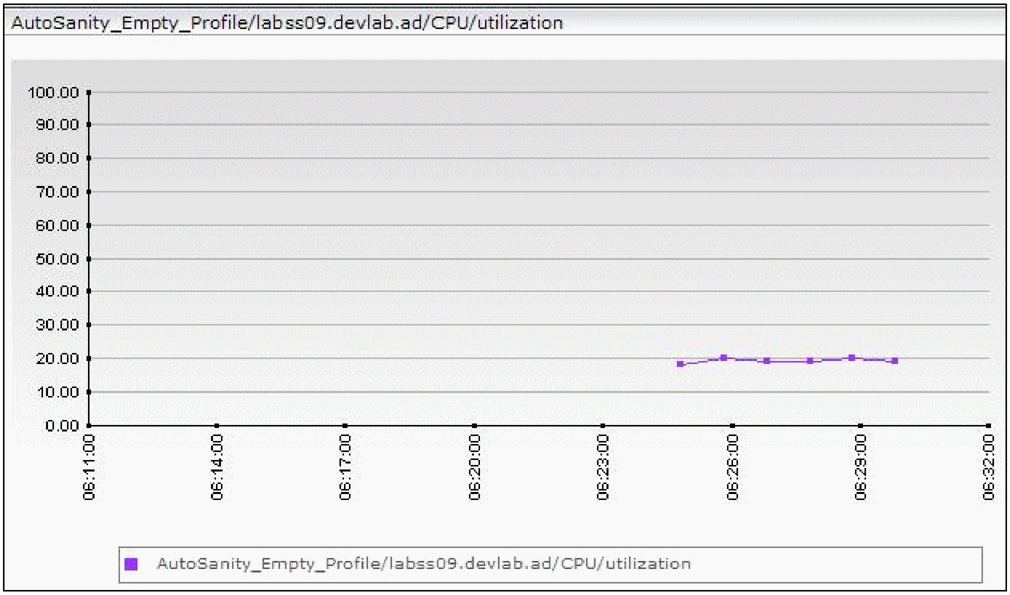
Note: If the data values of a monitor are outside the minimum or maximum configured values of the graph, the data points are displayed outside the boundaries of the graph.

To rescale the report, specify a minimum, a maximum, or both a minimum and a maximum value in the **Scale Min** and **Max** boxes.

For example, the original report displays as follows:



To rescale the range to 0-100, enter **0** in the Scale Min box and **100** in the Max box, or enter **100** in the Max box. The report redisplays as follows:



Examples

You can use the SiteScope Cross-Performance reports to identify a problem in a server. For example, select the SiteScope profile that refers to the SiteScope that samples the problematic server, select the relevant server, the monitor types (**CPU**, **memory**, and so on), the measurements that can help find the problem (**utilization**, **pages/sec**, **percent used**, and so on), and generate the report.

You can also compare memory usage in several servers. For example, select the SiteScope profile that refers to the SiteScope that samples the servers you want to compare, the relevant servers, the **memory** monitor type, the **pages/sec**, **percent used**, and **MB free** measurements, and then generate the report to compare the memory usage.

You can find out if a sub-system needs an additional server. For example, select the SiteScope profile that refers to the SiteScope that samples all servers in your sub-system, select all the servers of your sub-system, the **CPU** monitor type, the **utilization** measurements, and generate the report to see whether the sub-system needs an additional server.

Adjusting the Cross-Performance Report Scale

Measurement values in the cross-performance report are displayed along the y-axis using a normalized scale. By default, HP Business Availability Center automatically sets the scale factor for each measurement. If required, you can manually modify the scale factor for any measurement in the Selected Measurements table, for example, to better view multiple measurements whose data values span a wide range. For details, see “Rescaling a Cross-Performance Report” on page 115.

When you manually modify the scale factor, HP Business Availability Center scales measurement values by dividing the actual value by the value chosen in the scale list. Thus, a value of 100 with a scale setting of 0.1 is shown as 1000 along the y-axis. A value of 100 with a scale setting of 10 is shown as 10 along the y-axis.

For example, if at a given point in time Measurement A (whose scale value is set to “Auto”) has a value of 10 and Measurement B (whose scale value is set to 0.1) has a value of 90, the y-axis displays a range from 0-1000 to accommodate both values. If both measurements’ scale settings are set to “Auto,” the y-axis values ranges from 0-100.

Group Performance Report

You generate the Group Performance report and its subreports to view data that helps you spot trends in server performance that could lead to application performance problems. You can also analyze whether slow or failed transactions are being caused by server resource bottlenecks or other infrastructure machine-related problems.

This section includes the following topics:

- “Group Performance” on page 118
- “SiteScope Performance” on page 118
- “SiteScope Data Over Time” on page 120

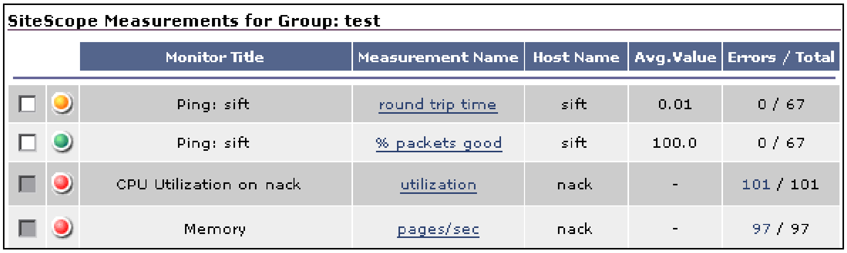
Group Performance

The Group Performance table is the top level of the report. For each group, the table displays a color-coded quality level, the number of subgroups, and the number of included measurements. The quality-level indicators enable you to see how monitors in the defined groups are performing. Click a group name to generate the SiteScope Performance subreport.

SiteScope Performance

The SiteScope Performance subreport displays a list of measurements collected by SiteScope for the specified group, over the selected time range. If the specified group contains subgroups, these are displayed at the top of the page. Click the subgroups to view their SiteScope Performance subreports.

The SiteScope Performance subreport displays the following information:



SiteScope Measurements for Group: test

		Monitor Title	Measurement Name	Host Name	Avg.Value	Errors / Total
□	🟠	Ping: sift	round trip time	sift	0.01	0 / 67
□	🟢	Ping: sift	% packets good	sift	100.0	0 / 67
▨	🔴	CPU Utilization on nack	utilization	nack	-	101 / 101
▨	🔴	Memory	pages/sec	nack	-	97 / 97

- **Check box.** An enabled check box at left indicates that there is monitor data that can be viewed in the SiteScope Data over Time report. For details on generating this report, see “SiteScope Data Over Time” on page 120.

- **Status.** The status column, to the left of the monitor title, displays measurement threshold icons, which indicate whether the average measurement is within the OK, Warning, or Error range, as reported by SiteScope. You define measurement thresholds for each measurement when you configure the monitor in the System Availability Management area in the Administration Console.

- **Monitor Title.** The monitor title.

- **Measurement Name.** The name of the measurement. Click the link to generate the SiteScope Data over Time report for that measurement. HP Business Availability Center displays the link only if data exists for the selected time range. For details on the SiteScope Data over Time report, see “SiteScope Data Over Time” on page 120.

- **Host name.** The name of the SiteScope host machine.

- **Avg. Value.** The average value of each listed measurement, or counter, for the specified time period.

- **Last Value (Updated).** The last received SiteScope measurement, as well as the most recent date and time that SiteScope received the measurement (shown in parentheses). HP Business Availability Center displays the date and time in italics if the current time frame is different from the displayed date and time.

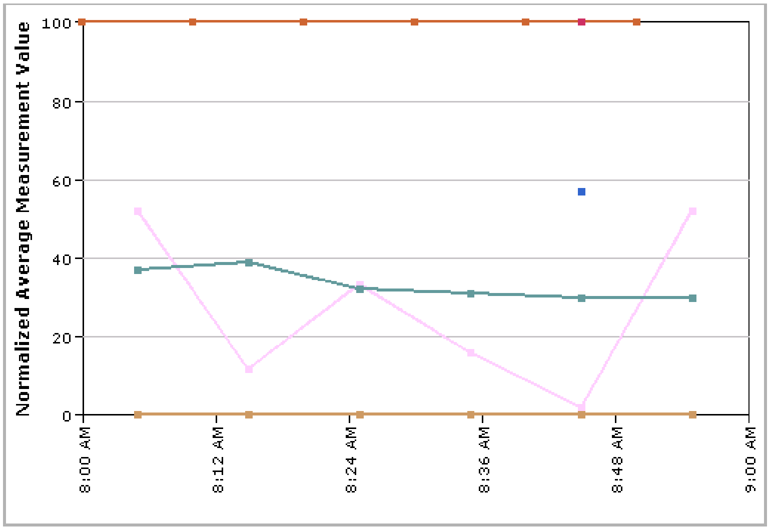
  If no value was collected within the past four hours, no value is displayed.

  If the last received SiteScope measurement returned the Error status, HP Business Availability Center displays the term Error in the Last Value (Updated) column.

- **Errors/Total.** The number of errors that occurred while collecting measurement data, out of the total number of measurements taken during the defined time period. Click the link to view a list of errors that returned measurement error messages. HP Business Availability Center displays the link only if errors occurred.

SiteScope Data Over Time

The SiteScope Data Over Time report displays specific measurement data over the selected time range. You can view this report for a single measurement, or for several measurements simultaneously.



Note: You can add the SiteScope Data over Time report to custom reports. For details, see “Custom Report Manager” in *Custom Reporting and Alerting*.

To view the SiteScope Data over Time subreport for one measurement:

1. Click a measurement in the **Measurement Name** column in the SiteScope Performance subreport. HP Business Availability Center generates and displays the SiteScope Data over Time subreport.
2. Place your cursor over a point in the graph to see a tooltip with measurement details.
3. Click the **View as Table** link to view the data in table format.

To view the SiteScope Data over Time subreport for several measurements:

1. In the SiteScope Performance subreport, select the check boxes beside the measurements that appear in the multi-measurement graph.
2. Click the **Generate** button at the bottom of the table. HP Business Availability Center generates and displays the multi-measurement SiteScope Data over Time subreport. You use the color codes to identify each measurement in the graph.

   The y-axis of the merged graph is a normalized scale from 0-100.
   HP Business Availability Center uses the following formula to convert the original y-axis value to a value in the merged y-axis:

   [original y-axis value] x [scale value] = y-axis value in merged graph

   Place the pointer over a point in the graph to view a tooltip with measurement details, including the measurement's original value.
3. Click the **View as Table** link to view the data in table format. The table displays actual measurement values, not normalized values.

Status Summary Report

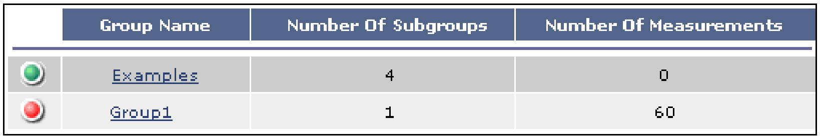
You generate the Status Summary report and its subreport to get an overall view of the performance of defined SiteScope groups and the monitors defined therein.

This section includes the following topics:

- "SiteScope Status Summary" on page 122
- "SiteScope Uptime Details" on page 122

SiteScope Status Summary

The SiteScope Status Summary table is the top level of the report. For each SiteScope group in the selected profile, the report displays a color-coded quality level, the number of subgroups, and the number of included measurements. The quality-level indicators enable you to get a quick snapshot of how monitors in the defined SiteScope groups are performing.

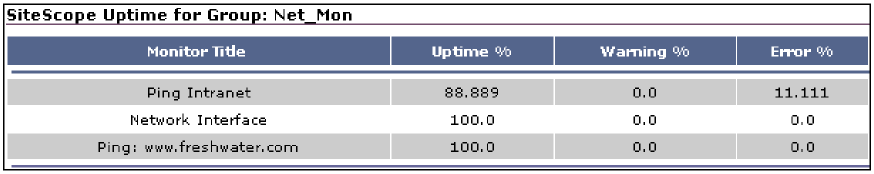


	Group Name	Number Of Subgroups	Number Of Measurements
🟢	Examples	4	0
🔴	Group1	1	60

Click a group name to generate the SiteScope Uptime Details subreport.

SiteScope Uptime Details

The SiteScope Uptime Details subreport displays OK, Minor, and Critical information for each monitor in the group, over the selected time range, enabling you to determine the overall performance trend of a given monitor. If the specified group contains subgroups, these are displayed at the top of the page. Click subgroups to view their SiteScope Uptime Details subreports.



SiteScope Uptime for Group: Net_Mon

Monitor Title	Uptime %	Warning %	Error %
Ping Intranet	88.889	0.0	11.111
Network Interface	100.0	0.0	0.0
Ping: www.freshwater.com	100.0	0.0	0.0

The SiteScope Uptime Details subreport displays the following data:

- **OK %.** The percentage of measurement instances that completed successfully.
- **Minor %.** The percentage of measurement instances whose values fell within the Minor threshold level.
- **Critical %.** The percentage of measurement instances whose values fell within the Critical threshold level.

Warning Summary Report

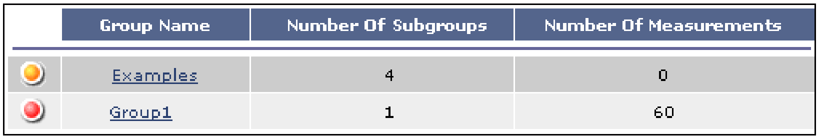
You generate the Warning Summary report and its subreport to identify the SiteScope groups whose measurements fell within the minor threshold level during the selected time period.

This section includes the following topics:

- "Warning Summary" on page 123
- "Warning Details Report" on page 124

Warning Summary

The Warning Summary table is the top level of the report. For each SiteScope group in the selected profile, the report displays a color-coded quality level, the number of subgroups, and the number of included measurements. The quality-level indicators enable you to get a quick snapshot of how monitors in the defined SiteScope groups are performing.

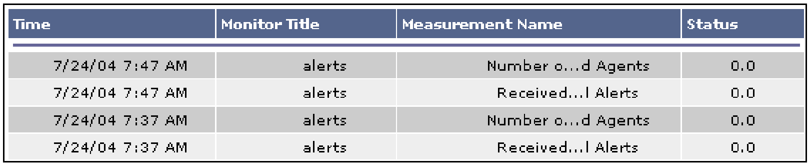


	Group Name	Number Of Subgroups	Number Of Measurements
🟠	Examples	4	0
🔴	Group1	1	60

Click a group name to generate the Warning Details subreport.

Warning Details Report

The Warning Details subreport displays minor status information for each measurement instance of each monitor in the group, over the selected time range. If the specified group contains subgroups, these are displayed at the top of the page. Click subgroups to view their SiteScope Warning Details subreports.



Time	Monitor Title	Measurement Name	Status
7/24/04 7:47 AM	alerts	Number o...d Agents	0.0
7/24/04 7:47 AM	alerts	Received...l Alerts	0.0
7/24/04 7:37 AM	alerts	Number o...d Agents	0.0
7/24/04 7:37 AM	alerts	Received...l Alerts	0.0

The Warning Details subreport displays the following data:

- **Time.** The date and time of the measurement instance.
- **Monitor Title.** The monitor to which the measurement is associated.
- **Measurement Name.** The measurement instance whose threshold fell within the Minor level.
- **Status.** The value of the measurement.

Note: System Availability Management displays raw data only in the SiteScope Warning Details report. Aggregated data is not used. Therefore, if raw historical data is removed from the profile database using the Purging Manager, you are unable to view data in the SiteScope Warning Details report for the time period for which the data was removed.

Error Summary Report

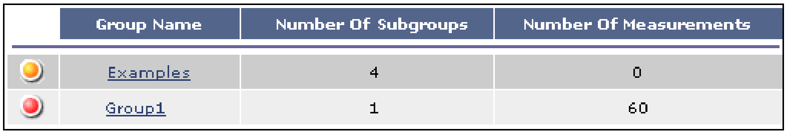
You generate the Error Summary report and its subreport to identify the SiteScope groups whose measurements fell within the critical threshold level during the selected time period.

This section includes the following topics:

- "Error Summary" on page 125
- "Error Details" on page 125

Error Summary

The Error Summary table is the top level of the report. For each SiteScope group in the selected profile, the report displays a color-coded quality level, the number of subgroups, and the number of included measurements. The quality-level indicators enable you to get a quick snapshot of how monitors in the defined SiteScope groups are performing.

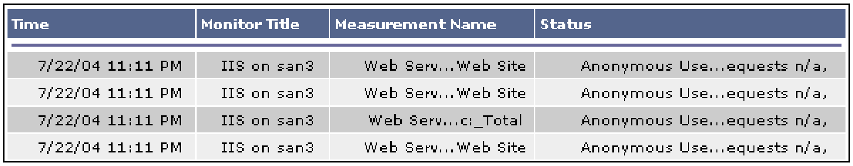


	Group Name	Number Of Subgroups	Number Of Measurements
●	Examples	4	0
●	Group1	1	60

Click a group name to generate the Error Details subreport.

Error Details

The Error Details subreport displays error status information for each measurement instance of each monitor in the group, over the selected time range. If the specified group contains subgroups, these are displayed at the top of the page. Click subgroups to view their Error Details subreports.



Time	Monitor Title	Measurement Name	Status
7/22/04 11:11 PM	IIS on san3	Web Serv...Web Site	Anonymous Use...equests n/a,
7/22/04 11:11 PM	IIS on san3	Web Serv...Web Site	Anonymous Use...equests n/a,
7/22/04 11:11 PM	IIS on san3	Web Serv...c:_Total	Anonymous Use...equests n/a,
7/22/04 11:11 PM	IIS on san3	Web Serv...Web Site	Anonymous Use...equests n/a,

The Error Details subreport displays the following data:

- **Time.** The data and time of the measurement instance.
- **Monitor Title.** The monitor to which the measurement is associated.
- **Measurement Name.** The measurement instance whose threshold fell within the Error level.
- **Status.** Error information as reported by SiteScope.

Note: System Availability Management displays raw data only in the SiteScope Error Details report. Aggregated data is not used. Therefore, if raw historical data was removed from the profile database using the Purging Manager, you are unable to view data in the SiteScope Error Details report for the time period for which the data was removed.

Set Group Permissions for Reports

Group permissions filters enable you to filter data for specific SiteScope groups or subgroups from System Availability Management reports, as well as the SiteScope Monitor Performance component in custom reports. When a user views a report, System Availability Management displays only the data from the groups and subgroups for which permissions are set. A user's ability to modify group permissions enables filtering data from reports that may be irrelevant to the specific user, making reports more manageable and increasing the speed of report generation.

This section includes the following topics:

- "Usage Privileges for Group Permission Filters" on page 127
- "Setting Group Permission Filters" on page 127

Usage Privileges for Group Permission Filters

Every HP Business Availability Center user can set personal group permission filters. Administrators can set group permission filters for other users, but each individual user can override those settings as required.

Users can apply group permission filters only to SiteScope profiles for which they have been granted permissions. When a user is assigned permissions for a SiteScope profile, group permission filters for that user are not enabled by default. Either the system administrator or the user must explicitly assign the required group permission filters. The user that originally connects to the SiteScope in System Availability Management is automatically assigned full group permissions. For details on granting permissions, see "Permissions Management" in *Platform Administration*.

Setting Group Permission Filters

You specify which SiteScope groups and subgroups to include in or filter from System Availability Management reports, for a specific SiteScope profile.

To set group permission filters:

1. From the **SiteScope Over Time Reports** tab in System Availability Management, select **Group Permissions for Reports** to open the SiteScope Group Permissions page.
2. Choose the user whose permissions you want to change.

   If you plan to apply the permissions to multiple users, this step is not required.
3. Choose the SiteScope profile from the list of profiles that the selected user has permission to view.

   HP Business Availability Center displays the SiteScope groups associated with the profile.

4 To make changes to the existing permissions:

- ➤ with the **Full Permission** check box cleared, select or clear the check boxes next to a group or subgroup. Click the expand (+) and collapse (-) symbols to reveal or hide the subgroups.
- ➤ select the **Full Permission** check box if you want the user to see data from all groups and subgroups. The user also sees data from any new monitors added to this group.
- ➤ clear the **Full Permission** check box, but leave all the group and subgroup check boxes selected, if you want the user to see all data, except the data from any new monitors that are added to the groups.

When you select a group, all its subgroups are also automatically selected. If you clear the check box of a group, the check boxes of all its subgroups are automatically cleared. This is because you cannot grant permissions for a user to view a subgroup, but not to view the parent group.

5 Click **Apply** to save the changes.

To apply specified permissions to multiple users, click **Apply Multiple Users**, select the users to which you want to apply permissions, and click **Apply**.

You can restore a previous configuration by clicking **Revert** before clicking **Apply**. Note also that if you move to another page before clicking **Apply**, the changes you made are not saved. When you return to this page, the previous configuration is displayed.

System Availability Management Data in Custom Reports

You can add System Availability Management reports to custom reports from the User Reports tab. For details, see "Custom Report Manager" in *Custom Reporting and Alerting*.

This section includes the following topics:

- "Monitor Performance Report" on page 129
- "SiteScope Data Over Time Report" on page 129
- "Group Performance Report" on page 129
- "Overall Performance Report" on page 130

Monitor Performance Report

To add this report to a custom report, select the SiteScope Monitor Performance component type in the Custom Report Manager. For details on the Monitor Performance report, see "Monitor Performance Report" on page 102.

SiteScope Data Over Time Report

To add this report to a custom report, select the Reports component type in the Custom Report Manager, then select the SiteScope Reports category from the Add Component dialog box. For details on the SiteScope Data over Time report, see "SiteScope Data Over Time" on page 120.

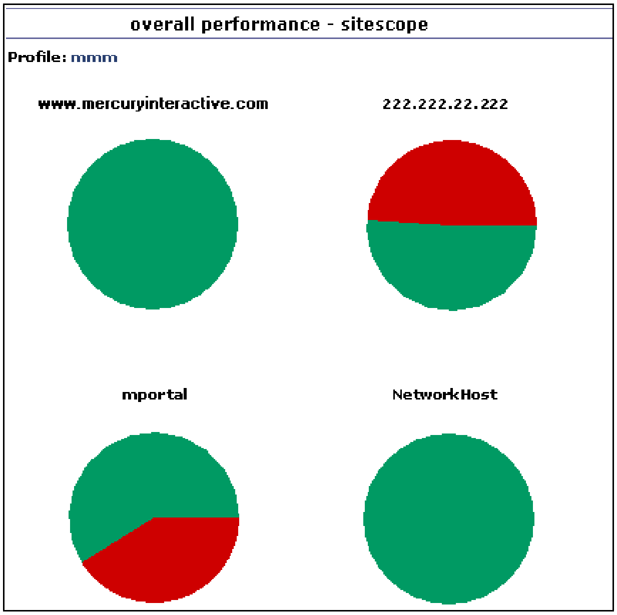
Group Performance Report

To add this report to a custom report, select the Reports component type in the Custom Report Manager, choose the SiteScope Reports category from the Add Component dialog box, then select SiteScope Profile Summary from the Type list. For details on the Group Performance report, see "Group Performance Report" on page 118.

Overall Performance Report

The Overall Performance report is based on SiteScope data, and is only available in custom reports. To add it to a custom report, select **Reports** in the **Component type** list in the Custom Report Manager page and click **Add Component**. Select the **SiteScope Reports** in the **Category** list from the Add Component dialog box, and then select **Overall Performance** in the **Type** list.

You view the Overall Performance report to get a quick snapshot of the performance of the monitored infrastructure machines in the selected SiteScope profiless. The chart displays—for the SiteScope profiles and defined time frame—a pie chart for each element of the infrastructure that SiteScope is monitoring.



To get additional information, point to a segment to view a tooltip describing the exact number and percentage of measurements for each segment of the chart.

7

The Event Log

The HP System Availability Management event log displays SiteScope events, as well as events collected from external applications or software by enterprise management systems (EMS) using SiteScope.

Note: The Event Log is available only to HP Business Availability Center users.

About the Event Log

The event log enables you to view event data over time, events that happened at a specific time, the details of a specific event, and (where possible) the event history.

The type of event that is collected depends on what is defined as an event in the external applications or software. Event types can be warnings, alerts, user logins, and so on.

The event log displays event data that is common to all data sources: the severity of the event, the application or software from which the event is collected, the time the event occurred, the hierarchy of the event source, the name (or the IP address) of the host or device that caused the event, the status or type of event, and the external system description of the event.

You can filter the events for a specific time frame, data source, severity, and target name. For details, see “Display and Customize the Event Log” on page 133.

You can then drill down to the common data to display data that is specific to the data source where the event occurred (for details, see “Working with Event Details” on page 138) and to display the history of a specific event (for details, see “Working with Event History” on page 140).

The event log enables you to diagnose specific issues in real time and to generate trend reports.

Display and Customize the Event Log

The Event Log page displays the logs of events that are sent to the system (for details, see "Displaying the Event Log" on page 133). You can use filters (time frame, data source, severity, and target name) to display specific information. If you select the SiteScope data source, you can then select additional filters: SiteScope profile, groups, and monitor type (for details, see "Set Additional Filters for SiteScope" on page 135).

When you generate the event log, the Event Log page displays the events sorted by the time of their occurrence in descending order. It also shows columns that are common to all the data sources that can send events (for details, see "Viewing Common Event Data in the Event Log Page" on page 136). The data of the SiteScope data source is filtered according to SiteScope Profile permissions (for details, see "Permissions Management" in *Platform Administration*).

The Event Log page has two areas: the filter and action area and the data table.

This section includes the following topics:

- "Displaying the Event Log" on page 133
- "Customizing Event Logs" on page 134

Displaying the Event Log

You can display the logs of events sent to HP Business Availability Center.

To display the Event Log:

1. Select **Applications** > **System Availability Management** > **Event Log** to display the Event Log page.
2. Select the time period for which you want to gather information to display in the report in the **View** list. For details, see "Choosing the Time Range and Granularity" in *Custom Reporting and Alerting*.

3 Click **Active Filters**, if you want to edit the filters. Only one or **All** data sources can be selected in the Event Source tab. If no data source exists, only **All** appears in the list. **SiteScopeAlert** or **SiteScopeStatusChange** data sources appear only if the current user has permissions to view at least one SiteScope profile. Severities are pre-defined. By default, all check boxes are selected.

If you select **SiteScopeAlert** or **SiteScopeStatusChange**, the SiteScope Filters window is displayed. For details, see “Set Additional Filters for SiteScope” on page 135.

4 Click one of the action buttons to print, e-mail, or open a report in Excel or PDF format. For details, see “Sharing and Storing Reports” in *Custom Reporting and Alerting*.

5 Click **Generate** to generate the report.

Note: If the number of events that occur during the specified time frame is larger than the maximum number of events that can be displayed in the report, a message is displayed. To reduce the number of events, select a more specific time range. For example, to see events for the past week, select the individual days of the week.

Customizing Event Logs

You can change the default setting of the maximum number of rows that can be displayed in the page. You can also change the maximum number of events that can be listed in the event log.

To change the maximum number of rows displayed in a page:

When there are too many events to display in one page of a table, a paging bar is automatically displayed.

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Application**, select **End User/System Availability**, and locate the **Max Table Rows** in the **Event Reports** table.

2 Modify the value to the required number of rows per page.

To change the maximum number of rows displayed in the Event Log:

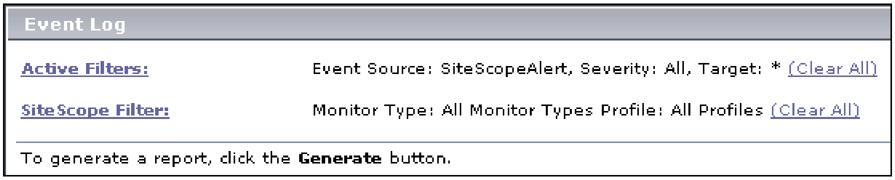
The maximum number of rows that can be displayed in the Event Log is 1000, by default.

1 Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Application**, select **End User/System Availability**, and locate the **Max Fetched Rows** in the **Event Reports** table.

2 Modify the value to the required number of rows per Event Log.

Set Additional Filters for SiteScope

If you select a SiteScope data source in the active filter, an additional filter is automatically provided to filter the data by SiteScope profile, group, and monitor type.



Event Log

Active Filters: Event Source: SiteScopeAlert, Severity: All, Target: * (Clear All)

SiteScope Filter: Monitor Type: All Monitor Types Profile: All Profiles (Clear All)

To generate a report, click the **Generate** button.

To work with additional filters for SiteScope data sources:

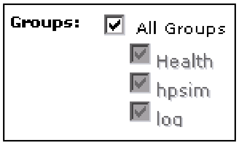
1 Click **SiteScope Filters**, to open the **SiteScope Filter** page.

2 Select the type of monitor in the **Monitor Type** list. The default is **All Monitor Types**.

3 Select the SiteScope profile in the **Profile** list. The default is **All Profiles**. To view events of interest regarding the profile or group permissions, select one of the profiles in the **Profile** list. The list of groups allowed for the selected profile is displayed. For details on profile or group permissions, see “Permissions Management” in *Platform Administration*.

Note: If you select **All Profiles**, your profile or group permissions are not applied to the displayed events.

4 If available, select the appropriate group in the group tree. Select **All Groups** if you want to select all the groups in the tree. When a tree CI changes its status (from selected to unselected or from unselected to selected) the status of the whole sub-tree changes.



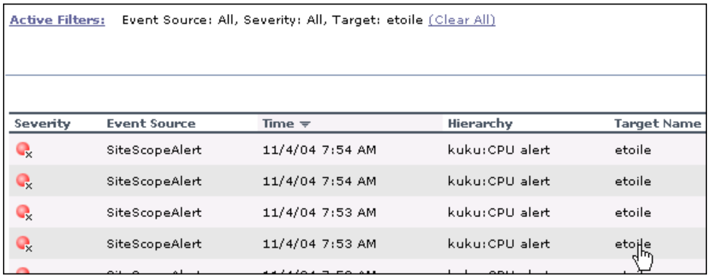
Groups: ☑ All Groups
- ☑ Health
- ☑ hpsim
- ☑ log

Viewing Common Event Data in the Event Log Page

The event data common to all event data sources is displayed in this table. The data is sorted by time in descending order.

To sort the report by a column, click the column title (an arrow appears in the column title to indicate whether the sort is descending or ascending).

Click a value in a specific row to add this selection to the active filter. The addition is reflected in the display.



Active Filters: Event Source: All, Severity: All, Target: etoile (Clear All)

Severity	Event Source	Time ▾	Hierarchy	Target Name
●	SiteScopeAlert	11/4/04 7:54 AM	kuku:CPU alert	etoile
●	SiteScopeAlert	11/4/04 7:54 AM	kuku:CPU alert	etoile
●	SiteScopeAlert	11/4/04 7:53 AM	kuku:CPU alert	etoile
●	SiteScopeAlert	11/4/04 7:53 AM	kuku:CPU alert	etoile

Each row in the table contains the data associated with one event:

- **Severity.** The icon and its tooltip display the severity of the event.

Icon	Severity
○	Unknown
🟢	Informational
🟢∿	Warning
🟡!	Minor
🟠‼	Major
🔴✕	Critical

- **Event Source.** The application or software from which the event is collected. Event sources can be: HP OVO, Remedy ARs, SitescopeAlert, SitescopeAlertStatusChange, Tivoli TEC, BMC Patrol, CA Unicenter, HP SIM, Compaq Insight Manager, Whatsup, or Compaq Insight Manager, depending on the external systems that sent the events to HP Business Availability Center.
- **Time.** The time when the event occurred. By default, the data sorted in this column is in descending order.
- **Hierarchy.** The hierarchy description of the event source. It can include the path to where the event occurred in the area, sub area, or instance and/or the event depending on the application or software from which the event is collected. Depending on the data source, the hierarchy can have two to four branches. If the hierarchy is very long, this field displays the shortened string and the tooltip displays the complete hierarchy.
- **Target Name.** The name or the IP address of the host or device that caused the event.
- **Status.** The status or type of the event. If the hierarchy is very long, the value is shortened and the tooltip displays the full hierarchy.

- **Description.** The event description. If the description is very long, the value is shortened and the tooltip displays the full hierarchy.

To view additional data for this event, click the **Event Details** button to open the Event Details page. For details, see “Working with Event Details” on page 138.

To view details about the event history data, click the **History** button to open the Event History page. For details, see “Working with Event History” on page 140.

Note: By default, some data sources include a history view and others do not (the History button is disabled or does not display). You can enable the history view by changing the setting in the Infrastructure Settings Manager. To modify the setting, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **End User/System Availability Management**, and locate the **Event Log Report Data Sources History** entry in the **End User/System Availability Management - Data** table. Set the property value by adding the data source names for which you want to enable the History button (separate data source names with commas)—in the Value box. The change takes place after restart. For details, see “Infrastructure Settings” in *Platform Administration*.

Working with Event Details

To display all the data (common and specific) related to an event, you display the event details.

Click the **Event Details** button in the Event Log page to open the Event Details report in a new window.

The Event Details report displays detailed information about the specified event as well as the fields and the field values from the event data. The type of information provided depends on the data source.

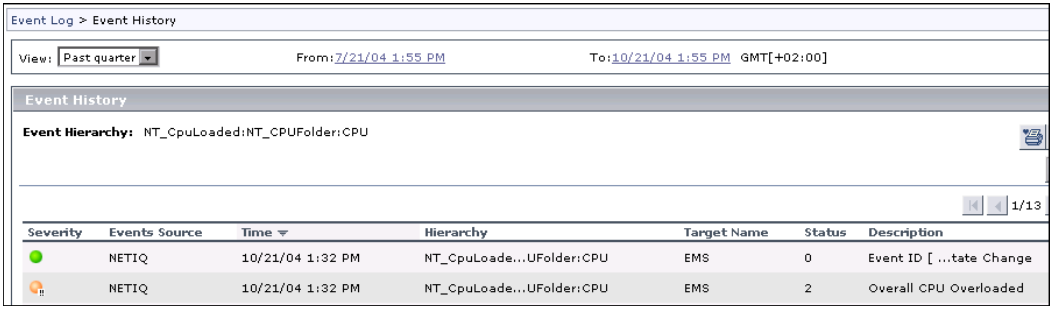
The Event Details report can display any of the following fields:

- **Time.** The time of the event.
- **Severity.** The severity of the event.
- **Original Severity.** The original severity of the event.
- **Status.** The event status or type. If the hierarchy is very long, this field displays a shortened string and the tooltip displays the complete status.
- **Event Source.** The application or software from which this event is collected.
- **Logical Group.** The additional logical level of event hierarchy
- **Hierarchy.** The hierarchy of the event source. It can include the path to where the event occurred in the area, sub area, or instance and/or the event depending on the application or software from which the event is collected.

  Depending on the data source, the hierarchy can have two to four branches. If the hierarchy is very long, this field displays the shortened string and the tooltip displays the complete hierarchy.
- **Target Name and IP.** The name or IP address of the host or device that caused this event.
- **Collector host.** The name of the machine that collected the data.
- **Description.** A description of the event.
- **Acknowledged By.** The operator who acknowledged this event.
- **Value.** Any numeric values that are sent with the event.
- **Additional information field (1... 5).** Additional rows (up to 5) that contain additional information for the current event.

Working with Event History

Click the **Event History** button in the Event Log page to open the Event History report in a new window.



Event Log > Event History

View: Past quarter From: 7/21/04 1:55 PM To: 10/21/04 1:55 PM GMT[+02:00]

Event History

Event Hierarchy: NT_CpuLoaded:NT_CPUFolder:CPU

1/13

Severity	Events Source	Time	Hierarchy	Target Name	Status	Description
●	NETIQ	10/21/04 1:32 PM	NT_CpuLoade...UFolder:CPU	EMS	0	Event ID [...tate Change
●	NETIQ	10/21/04 1:32 PM	NT_CpuLoade...UFolder:CPU	EMS	2	Overall CPU Overloaded

The Event History report displays detailed information about the specified event for different time periods.

The data displayed provides a historical view of the event:

- **Event Source.** The application or software from which the event was collected. Event sources can be: HP OVO, Remedy ARs, SitescopeAlert, SitescopeAlertStatusChange, Tivoli TEC, BMC Patrol, CA Unicenter, HP SIM, Compaq Insight Manager, Whatsup, or Compaq Insight Manager, depending on the external systems that sent the events to HP Business Availability Center.
- **Time.** The time when the event occurred. By default, the data sorted in this column is in descending order.
- **Hierarchy.** The hierarchy description of the event source. It can include the path to where the event occurred in the area, sub area, or instance and/or the event depending on the application or software from which the event was collected. Depending on the data source, the hierarchy can have two to four branches. If the hierarchy is very long, this field displays the shortened string and the tooltip displays the complete hierarchy.
- **Target Name.** The name or the IP address of the host or device that caused the event.
- **Status.** The status or type of the event. If the hierarchy is very long, the value is shortened and the tooltip displays the full hierarchy.

➤ **Description.** The event description. If the description is very long, the value is shortened and the tooltip displays the full hierarchy.

To view different periods of the event history select the appropriate time frame in the **View** list. This selection has no effect on the time frame selected in the **View** list in the Event Log page.

Note: By default, some data sources include a history view and others do not (the History button is disabled or does not display). You can enable the history view by changing the setting in the Infrastructure Settings Manager. To modify the setting, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, click **Applications**, select **End User/System Availability Management**, and locate the **Event Log Report Data Sources History** entry in the **End User/System Availability Management - Data** table. Set the property value by adding the data source names for which you want to enable the History button (separate data source names with commas)—in the Value box. The change takes place after restart. For details, see “Infrastructure Settings” in *Platform Administration*.

8

User Reports

User reports is a feature common to the HP Business Availability Center applications. You configure and view user reports from the User Reports tab.

For complete details on creating, viewing, and administering user reports, see “User Reports” in *Custom Reporting and Alerting*.

Note: The User reports feature is available only to HP Business Availability Center users.

Part II

SiteScope General and Administration

9

SiteScope Monitor Tree

This chapter includes the main concepts and tasks for the SiteScope monitor tree.

SiteScope Monitor Tree Overview

SiteScope monitors are individually configured instruction sets that automatically test performance and availability of systems and services in the network environment. SiteScope monitoring includes alerting and reporting capabilities, along with a dashboard for a real-time picture of the monitored environments.

SiteScope's interface objects are organized into a hierarchy represented by a monitor tree. You use the monitor tree to navigate through containers and elements in SiteScope and drill down to monitor and other configuration settings. For details on the different hierarchy elements, see "Monitor Tree" on page 153.

You can customize your view of the monitor tree to list only those SiteScope elements with which you are working. You can also assign categories to your groups, monitors, reports, and alerts to further refine your selection. For details, see “Setting Views and Defining Categories” on page 171.

SiteScope enables you to change monitor configurations across multiple monitors, groups, or multiple SiteScopes using Global Replace. For details, see “Global Search and Replace Wizard” on page 279.

SiteScope Monitors and HP Business Availability Center Configuration Items

If your SiteScope is integrated with HP Business Availability Center, when you create a monitor, that monitor object creates a corresponding configuration item (CI) in the Universal configuration management history database. For details on understanding configuration items, see “Configuration Management Database (CMDB) Concepts” in *Reference Information*.

The monitors that populate the CMDB are represented in the CMDB as monitor CIs. Monitor CIs receive data from the SiteScope monitor and use the data to calculate Key Performance Indicator status.

You can also create relationship between a monitor and any existing, logical CI in the CMDB. This relationship enables the monitor to pass KPI status to the CI to which it is attached.

You can create this relationship:

- using the **Modeling** tab in Universal CMDB Administration. For details, see “Attaching Existing CIs” in *IT World Model Management*.
- using the **Link Monitor to CI** area while creating a monitor. The **Select CIs** button in this area opens the Select CIs dialog box in which you can select a view in the left pane that includes the CI you want to attach to the monitor. For details on selecting and working with views, see “View Explorer” in *Reference Information*.

- using the **Monitor Deployment Wizard** to deploy SiteScope monitors onto existing CIs. If a SiteScope monitor already has an attached CI, you can use the Monitor Deployment Wizard to modify the monitors that are reporting status to the attached CI. For details, see "Monitor Deployment Wizard Concepts and Tasks" on page 59.

Note: The Monitor Deployment Wizard is available only to those users accessing SiteScope using System Availability Management Administration in HP Business Availability Center.

You can view and edit the relationship you created in the IT Universe tab in CMDB Administration.

Note: The monitor CI appears in the views as a child object to the original CI only if, in the original CI's properties, the **Include Related Elements** option is selected. For details, see "Include Related CIs" in *IT World Model Management*.

Copying and Moving SiteScope Objects

You can copy SiteScope objects to different locations in the monitor tree. In addition, you can move a monitor or monitor group and its contents to a template or to a different monitor group.

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

You can copy or move the following SiteScope objects:

Context Menu Option	**Action**	**Description**
Monitor group	Cut/Paste Copy/Paste	Enables you to copy or move a monitor group, including its monitors, alerts, and reports. You can make a copy in the same monitor group, or copy or move it to a different monitor group. You can also copy it to a different template. **Note:** You cannot move or copy a monitor group to its subgroup.
Monitor	Cut/Paste Copy/Paste	Enables you to copy or move a monitor, including its alerts and reports. You can make a copy in the same monitor group, or copy or move it to a different monitor group. You can also copy it to a different template.
Template Container	Paste	Enables you to paste a template into the template container.
Template	Copy/Paste	Enables you to copy a template group or template monitor to a template container or template.
Alert	Copy/Paste	Enables you to copy the alert to another location in the monitor tree.
Report	Copy/Paste	Enables you to copy the report to another location in the monitor tree.

For details on copying or moving SiteScope objects, expand the relevant context menu option in “Context Menu Options” on page 158.

Navigating and Performing Actions in the Contents Tab and the Monitor Tree

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

The monitor tree itself enables you to highlight any object within the tree and right-click the object to access a menu of options for that object. For example, if you right-click the SiteScope node, you select from a menu listing only those actions that can performed on the SiteScope node.

The Contents tab enables you to view all the objects within any of the containers or profiles in the monitor tree, including the SiteScope node itself. When an object that includes child objects is highlighted, the Contents tab lists all of the child objects according to their type.

Additionally, the Contents tab enables you to select actions for each object type. The actions applicable to the highlighted object appear as optional buttons at the top of the Contents page. The actions applicable to the child objects of the highlighted object appear as optional buttons in the area listing the objects of that type.

Accessing Object Properties for Editing

You can select from the following options when accessing an object's properties for editing:

- In the monitor tree, right-click the object and choose **Edit** in the profile's menu.
- In the Contents tab you can either:
  - highlight the appropriate object in the monitor tree and click the **Edit** button at the top of the Contents page.
  - click the **Edit** button next to the appropriate object where it appears under object type in the Contents page.

10

Monitor Tree User Interface

This chapter includes a description of the pages and dialog boxes that are part of the Monitor Tree user interface.

Monitor Tree

Description	The monitor tree of SiteScope represents the organization of systems and services in your network environment. The tree includes containers and objects within your infrastructure.
Important Information	The root node of the tree is the SiteScope container. Only one SiteScope node exists in the monitor tree. You add all other elements to the tree under the SiteScope node.

Monitor Tree View Options

Menu Item	Description
Monitor	To filter the objects appearing in the monitor tree by monitor name, enter a monitor name and press ENTER. ➤ The monitor name is the string entered in the **Name** field in the Main Settings area during monitor configuration. ➤ Clear the field and press ENTER to clear the filter. ➤ Enter a regular expression to widen the filter. The monitor tree displays only those monitors, within their groups, matching the string entered and only those groups containing these monitors. **Example**: To display only those monitors beginning with the string CPU, enter CPU* and press ENTER.
Target	To filter the objects appearing in the monitor tree by the target server, enter a server name and press ENTER. ➤ The target is the string entered in the **Server** field in the Main Settings area during monitor configuration. ➤ Clear the field and press ENTER to clear the filter. ➤ Enter a regular expression to widen the filter. The monitor tree displays only those monitors, within their groups, whose target server matches the string entered and only those groups containing these monitors.
View window	Select an existing view from the drop-down list. You create views in the Views tab to modify the objects that appear in the monitor tree. For details, see "Defining and Managing View Settings" on page 172.

Monitor Tree Objects

The Monitor Tree includes the following elements:

GUI Element	Description
📁	Represents an individual SiteScope server. **Parent:** Enterprise node or container. **Add to tree by:** Importing or adding an empty SiteScope profile.
📁	Represents a template container. A template container is used to organize configuration deployment templates. For details, see "Using Templates to Deploy SiteScope Monitoring" on page 1069. **Parent:** SiteScope. **Add to tree by:** Creating, or importing with a SiteScope that has template containers defined.
📁	Represents a solution template container. **Parent:** SiteScope.
□	Represents a template configuration for deploying SiteScope objects. **Parent:** Template container. **Add to tree by:** Creating.
x	Represents a variable used as placeholder to prompt for input when deploying a template. **Parent:** Template. **Add to tree by:** Creating.
⬚	Represents a SiteScope monitor group or subgroup. **Parent:** SiteScope or SiteScope group. **Add to tree by:** Creating, or importing with a SiteScope that has groups defined.

GUI Element	Description
🖥	Represents a SiteScope monitor. **Parent:** SiteScope group or subgroup, template, or solution template. **Add to tree by:** Creating, or importing with a SiteScope that has monitors configured.
📁	Preferences representing the collection of SiteScope configuration settings. **Parent:** SiteScope. **Add to tree by:** Creating, or importing with a SiteScope that has preferences defined.
📝	Represents a preference. **Parent:** Preferences container or preference.
🖥	Represents a remote server preference. **Parent:** Preferences container, remote server preference, or template. **Add to tree by:** Creating.
♥	Represents the collection of available health monitors that are deployed to check proper functioning of SiteScope monitors. **Parent:** SiteScope. **Add to tree by:** Automatically added with SiteScope object.
⚡	Represents the collection of alert schemes configured for the SiteScope. **Parent:** SiteScope. **Add to tree by:** Automatically added with SiteScope object.

GUI Element	Description
⚠	Represents an alert. **Parent:** SiteScope, SiteScope group container, a template, or a monitor. **Add to tree by:** Creating.
📄	Represents a report. **Parent:** SiteScope, SiteScope group container, or a monitor. **Add to tree by:** Creating.
📁	Represents a tools container. A container used to organize the various tools for configuring the SiteScope. **Parent:** SiteScope.
⟳	Click the **Refresh** button to refresh the data in the tree.
|◂	Click the **Hide Tree Panel** button to hide the Monitor Tree and expand the right pane.

Context Menu Options

Following are descriptions of the various context menu options that are available for each object in the monitor tree.

SiteScope Context Menu Options

Menu Item	Description
Expand All	Opens all the subtrees under SiteScope.
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see "Global Search and Replace Wizard" on page 279.
Monitor Deployment Wizard	Opens the Monitor Deployment Wizard. For details, see "Monitor Deployment Wizard Concepts and Tasks" on page 59.
New Alert	Opens the New Alert window which enables you to define a new alert for SiteScope.
New Group	Opens the New Group window which enables you to define a new SiteScope group.
New Report	Opens the New Report window which enables you to define a new SiteScope report.
New Template Container	Opens the New Template Container window which enables you to define a new template container.
Paste	Pastes the selected SiteScope object (that was previously copied or cut) to the SiteScope node.
Paste from other SiteScope	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Pastes the selected SiteScope object (that was previously copied or cut) from another SiteScope to the SiteScope node.

Template Container Context Menu Options

Menu Item	Description
Delete	Deletes the template container.
Edit	Opens an editing window for the template container, which enables you to edit its settings.
Expand All	Expands the templates container to display all the template objects within the container.
Export	Opens the Export Template window which enables you to export a template file.
Import	Opens the Import Template window which enables you to import a template file.
New Template	Opens the New Container window which enables you to define a new template.
New Template Container	Opens the New Template Container window which enables you to define a new template container.
Paste	Pastes a template into the template container.

Solution Templates Context Menu Options

Menu Item	Description
Expand All	Expands the solution templates container to display all the solution templates within the container.

Template Context Menu Options

Menu Item	Description
Copy	Copies a template group, monitor, or alert. You can paste the template group, monitor, or alert to the SiteScope tree.
Delete	Deletes the template.
Edit	Opens an editing window for the template, which enables you to edit its settings.
Expand All	Opens all the subtrees under the template.
New Alert	Opens the New Alert window which enables you to define a new alert for the template.
New Group	Opens the New Group window which enables you to define a new template group.
New Monitor	Opens the New Monitor window, which enables you to define a new monitor.
New Remote NT	Opens the New Template window, which enables you to define a new remote NT template.
New Remote Unix	Opens the New Template window, which enables you to define a new remote UNIX template.
New Variable	Opens the New Template Variable window, which enables you to define a new template variable.
Paste	Pastes a template group, monitor, or alert to a template.

Template Variable Context Menu Options

Menu Item	Description
Delete	Deletes the template variable.
Edit	Opens an editing window for the template variable, which enables you to edit its settings.

Group Context Menu Options

Menu Item	Description
Copy	Copies the group and its contents (monitors, alerts, and reports) to a monitor group or template.
Copy to other SiteScope	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Copies the group and its contents (monitors, alerts, and reports) from another SiteScope to a monitor group or template in the SiteScope node.
Cut	Moves the group and its contents (monitors, alerts, and reports) or a monitor and its contents (alerts and reports) to a monitor group.
Delete	Deletes the group.
Edit	Opens an editing window for the group, which enables you to edit its settings.
Expand All	Opens all the subtrees under the group.
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see "Global Search and Replace Wizard" on page 279.
Monitor Deployment Wizard	Opens the Monitor Deployment Wizard. For details, see "Monitor Deployment Wizard Concepts and Tasks" on page 59.
New Alert	Opens the New Alert window which enables you to define a new alert for the group.
New Group	Opens the New Group window which enables you to define a new SiteScope group.
New Monitor	Opens the New Monitor window which enables you to define a new SiteScope monitor.
New Report	Opens the New Report window which enables you to define a new SiteScope report.

Menu Item	Description
Paste	Pastes the selected group and its contents (monitors, alerts, and reports) or a monitor and its contents (alerts and reports) to the specified monitor group.
Paste from other SiteScope	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Pastes the selected group and its contents (monitors, alerts, and reports) or a monitor and its contents (alerts and reports) from another SiteScope to the specified monitor group.
Run Monitors	Runs any monitors configured in the group, and opens an information window with the results.

Monitor Context Menu Options

Menu Item	Description
Copy	Copies the monitor and its contents (alerts and reports) to a monitor group or template.
Copy to other SiteScope	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Copies the monitor and its contents (alerts and reports) from another SiteScope to a monitor group or template.
Cut	Moves the monitor and its contents (alerts and reports) to a monitor group.
Delete	Deletes the monitor.
Edit	Opens an editing window for the monitor, which babels you to edit its settings.
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see "Global Search and Replace Wizard" on page 279.
New Alert	Opens the New Alert window which enables you to define a new alert for the monitor.
New Report	Opens the New Report window which enables you to define a new SiteScope report.
Paste	Pastes the selected monitor context object to the specified monitor.
Paste from other SiteScope	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Pastes the selected monitor context object from another SiteScope to the specified monitor.
Run	Runs the monitor and opens an information window with the results.

Preferences Context Menu Options

Menu Item	Description
Expand All	Opens all the subtrees under the preferences.
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see "Global Search and Replace Wizard" on page 279.

Preference Context Menu Options

Menu Item	Description
<context-sensitive options>	The context menu options for a preference object are specific to the individual preference.

Server Preference Context Menu Options

The following options are available for the Preferences container only. They are not available for individual preferences.

Menu Item	Description
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see "Global Search and Replace Wizard" on page 279.
New Windows/UNIX Server	Opens the New Server window which enables you to define a new Windows or UNIX server.

SiteScope Health Context Menu Options

Menu Item	Description
Disable Logging	Disables logging on SiteScope Health. For details, see "Monitoring SiteScope Server Health" on page 293.
Enable Logging	Enables logging on SiteScope Health. For details, see "Monitoring SiteScope Server Health" on page 293.
Expand All	Opens all the subtrees under SiteScope Health.
New Alert	Opens the New Alert window which enables you to define a new alert for Health.
New Group	Opens the New Group window which enables you to define a new SiteScope group.
New Monitor	Opens the New Monitor window which enables you to define a new SiteScope monitor.
New Report	Opens the New Report window which enables you to define a new SiteScope report.
Paste	Pastes monitors and monitor groups into the Health container.
Run Monitors	Runs the health monitors and opens an information window with the results.

Alert Context Menu Options

Menu Item	Description
Copy	Copies the alert to the selected location in the monitor tree.
Copy to other SiteScope	This menu item is available only through System Availability Management Administration when there is more than one SiteScope connected to Business Availability Center. Copies the alert from another SiteScope to the selected location in the monitor tree.
Delete	Deletes the alert.
Disable	Disables the alert.
Edit	Opens an editing window for the alert, which enables you to edit its settings.
Enable	Enables the alert.
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see "Global Search and Replace Wizard" on page 279.
Test	Opens the Test Alert page which enables you to test the alert.

Reports Context Menu Options

Menu Item	Description
Copy	Copies the report to the selected location in the monitor tree.
Delete	Deletes the report.
Edit	Opens an editing window for the report, which enables you to edit its settings.
Global Replace	Opens the Global Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details, see "Global Search and Replace Wizard" on page 279.

Tools Context Menu Options

Menu Item	Description
Expand All	Opens all the subtrees under Tools.

Contents Tab

Description	Displays view panels and tables that enable you to view the current status of monitors, view the detailed content of object containers, and manage configuration settings for monitors, alerts, and reports. **To access:** Select an object and click the Contents tab in the right pane.
Important Information	The Contents tab enables you to view all the objects within any of the containers or profiles in the monitor tree, including the SiteScope node itself. When an object that includes child objects is highlighted, the Contents tab lists all of the child objects according to their type. Additionally, the Contents tab enables you to select actions for each object type. The actions applicable to the highlighted object appear as optional buttons at the top of the Contents page. The actions applicable to the child objects of the highlighted object appear as optional buttons in the area listing the objects of that type.

The Contents Tab includes the following elements:

GUI Element	Description
Up	Click to go up one level in the Monitor Tree. This option is not available for SiteScope (the highest level in the tree).
<action buttons>	The Contents tab for each of the objects contains action buttons corresponding to the context menu options in the Monitor Tree for that object. For details, see the relevant context menu options under "Monitor Tree" on page 153.

The Contents Tab for each object contains areas specific to that object as follows:

Object	Child Objects
SiteScope	Template Containers Groups Preferences Health Alerts Reports Tools
Template Container	Template Containers Templates
Template	Template Groups Template Alerts Template Monitors Template Variables Template UNIX Remote Template NT Remote
Group	Groups Alerts Reports Monitors
Monitor	Alerts Reports

Object	Child Objects
Preferences	General Settings UNIX Server Container Log Preferences E-mail Recipient Container Pager Recipient Container SNMP Trap Container Dynamic Update Container Absolute Schedule Container Infrastructure Settings Preferences Windows Server Container Range Schedule Container Users
Server Preferences	Servers
Health	Groups Alerts Reports Monitors
Tools	The selection of tools available for monitoring.

11

Views and Categories

This chapter includes the main concepts and tasks for Views and Categories.

Setting Views and Defining Categories

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

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

You can also assign categories to any object in the monitor tree and use those categories to filter the view. For example, you define a category for all monitors running on a specific operating system.

For details on views, see the next section.

For details on categories, see “Working with Categories” on page 173.

Defining and Managing View Settings

You define and manage view settings by accessing the Views tab at the top of the SiteScope interface.

You can define views:

- **based on object type only.** For example, you can define a view that includes all CPU monitors, regardless of their properties. In this view, the monitor tree lists all the CPU monitors defined in the SiteScope.
- **based on object type and the properties configured for the selected object types.** For example, you can define a view that includes all SiteScope monitors with the same host defined, giving you a view of only those monitors monitoring the selected host.
- **to appear in a flat list.** A flat list lists all objects meeting the view's selection criteria as child objects to the SiteScope node, regardless of its parent object.
- **to appear as a hierarchy.** The hierarchy option lists all objects with their respective parent objects even if the parent object does not meet the view's selection criteria.
- **to include all child objects of a selected object.** This is done by making your selections recursively.
- **to represent object properties.** This is done by using regular expressions to represent object properties if basing your selections on an object's properties.

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

Working with Categories

You create custom categories for use in filtering the display of the monitor tree for your monitor deployment. You define the categories and their values, and assign these to the different elements in your enterprise.

For example, you define a category called Priority with the possible values of Critical, High, Medium, and Low. You assign these category values to different elements in the infrastructure. Monitors of Web servers and databases that support 24x7 customer access could be assigned a category value of Priority: Critical. While adding a new view setting, you select types in the Filter by Types area, and click **Apply Selection**. In the Filter by Property Values area, expand the **Category Settings** area, select the **Assigned categories** check box, and select Priority:Critical as the value of the object. This filter displays only those elements to which you assigned this category and value.

Create and Define a New Category

The following workflow describes how to define a new category and assign it to one or more elements in the monitor tree:

Create a Category

You use the Categories area of SiteScope to add categories. For details, see “Categories Page” on page 179.

Assign Categories to Monitor Tree Elements

Before you can use a category as part of a view filter, you must assign the category to one or more elements in the monitor tree. You can assign categories to any item in the tree, including any container, monitor, group, alert, profile, or preference.

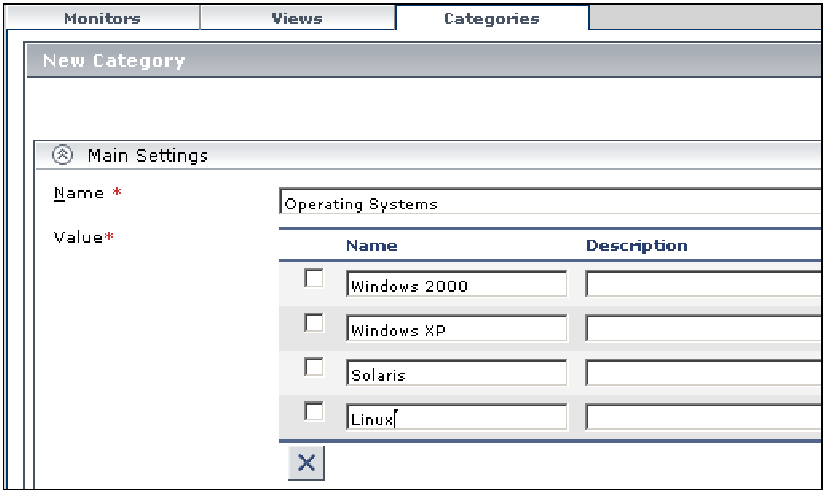
You assign categories while adding, importing, or editing objects in the monitor tree. **Category Settings** are included as properties for every type of object in the monitor tree.

Define a Category for a View Setting

Once you have assigned the category to one or more items in the monitor tree, you can use the category as an object for a view filter.

Example

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



Name * Operating Systems

Value*

	Name	Description
□	Windows 2000	
□	Windows XP	
□	Solaris	
□	Linux	

Assign the category to a monitor tree element such as a group by editing it and selecting Operating Systems as an Assigned category under **Category Settings**.

Using this new category, you could define a view setting for the monitor tree to display only those monitors running on Linux machines.

12

SiteScope Views and Categories User Interface

This chapter includes a description of the pages and dialog boxes that are part of the SiteScope Views and Categories user interface.

Views Page

Description	Enables you to add and edit views. **To access:** Click the **Views** tab in SiteScope.
Important Information	The Views page lists all the views that have been defined for the monitor tree. Two default views, Alerts and Reports, are automatically defined on the page.
Useful Links	“Views and Categories” on page 171

The Views page includes the following elements (listed alphabetically):

GUI Element	Description
✎	Click **Edit** to open the Edit View page which enables you to edit the selected view.
☑	Click **Select All** to select all the views.
□	Click **Select None** to clear all the selections.
⇄	Click **Invert Selection** to switch the selected views with the unselected ones.
✕	Click **Delete** to delete the selected views.
Description	A description of the view.
Name	The name of the view.
New View	Click **New View** to open the New View page which enables you to define a new view.

New View/Edit View Page

Description	Enables you to add a new view or edit an existing one. **To access:** Click the **New View** button or the **Edit** button from the Views page.
Useful Links	"Views and Categories" on page 171

The Main Settings area of the New View/Edit View page includes the following elements (listed alphabetically):

GUI Element	Description
?	Click the **Show Descriptions** button to display additional information about the dialog box elements.
Name	Enter a view filter name in the **Name** field. This name appears in the list of available views above the monitor tree.
Result Type	Select whether you want your view to appear as a flat list or in a hierarchy.

The Filter by Types area of the New View/Edit View page includes the following elements (listed alphabetically):

GUI Element	Description
⧉	Click **Select None** to clear all the selections.
<SiteScope objects>	Select the check box to the left of the object by which you want to filter your view. You can select multiple objects. When you apply your selection, the Filter by Property Values area is updated to accord with the objects you select.
Apply Selection	Click **Apply Selection** to apply the settings you selected.
Recursive Selection	Select **Recursive Selection** to automatically select all child objects of a selected object. **Note:** If you have selected **Recursive Selection** and want to remove a selected object from the selection, you must clear the selection of the object which you do not want to appear in the view and clear **Recursive Selection**. If you do not clear **Recursive Selection**, all objects within that parent object appear in the view even if you have cleared that object from the selection.

GUI Element	Description
Show all properties (Advanced)	Select the **Show all properties** option to display in the Filter by Property Values area all properties associated with all the object types selected in this Filter by Types list.
Show shared properties	Select the **Show shared properties** option to display in the Filter by Property Values area only those properties that are shared by all the object types selected in this Filter by Types list.

The Advanced area of the New View/Edit View page includes the following element:

GUI Element	Description
Description	You can expand the Advanced Settings area and enter a description for the category. This description appears only when editing the category. **Note:** This field is optional

The Filter by Property Values area of the New View/Edit View page includes the following element:

GUI Element	Description
<SiteScope object properties>	The Filter by Property Values area includes the properties specific to the SiteScope objects selected in the Filter by Types area. Enter or select a value for each property by which you want to filter.

Categories Page

Description	Enables you to add and edit categories. **To access:** Click the **Categories** tab in SiteScope.
Useful Links	"Views and Categories" on page 171

The Categories page includes the following elements (listed alphabetically):

GUI Element	Description
✎	Click **Edit** to open the Edit Category page which enables you to edit the selected category.
☑	Click **Select All** to select all the categories.
□	Click **Select None** to clear all the selections.
⇄	Click **Invert Selection** to switch the selected categories with the unselected ones.
✕	Click **Delete** to delete the selected categories.
Description	A description of the category.
Name	The name of the category.
New Category	Click **New Category** to open the New Category page which enables you to define a new category.

New Category/Edit Category Page

Description	Enables you to add a new category or edit an existing one. **To access:** Click the **New Category** button or the **Edit** button from the Categories page.
Useful Links	“Views and Categories” on page 171

The New Category/Edit Category page includes the following elements (listed alphabetically):

GUI Element	Description
?	Click the **Show Descriptions** button to display additional information about the dialog box elements.
☒	Click **Delete** to delete a selected value.
Advanced Settings - Description	You can expand the Advanced Settings area and enter a description for the category. This description appears only when editing the category. **Note:** This field is optional.
Name	Enter a new category name in the **Name** field. This name appears as the display name in the Categories page, and when defining or editing category settings for all objects in the monitor tree.
New Value	Click to add a row for entering a new value for the category.
Value Description	Enter an optional description for each value. This description appears only when editing the category.
Value Name	Enter a name for the value to be included in the category. Each category must include at least one value. Each value appears as a child object of the category name when defining or editing category settings for all objects in the monitor tree.

13

Preferences

This chapter includes the main concepts and tasks of SiteScope monitors preferences.

SiteScope General Preferences Overview

This section includes the main concepts of SiteScope General Preferences.

Working in an Internationalization Environment

SiteScope supports working in an internationalization environment.

This section includes the following topics:

- "General Limitations" on page 182
- "Multi-Lingual User (MLU) Interface Support" on page 183
- "Database Environment Issues" on page 184
- "Monitors Tested for Internationalization" on page 184

General Limitations

- Username, password, and URLs must be in English characters.
- Support for internationalization is available only in the new user interface.
- The machine on which SiteScope is installed (SiteScope machine) and the monitored machine must have the same locale. English is the default locale.
- The SiteScope machine can have a non-English locale in addition to English. For example, the monitored machine supports the German locale while the SiteScope machine supports German and English. For details on setting a non-English locale, see "Configure SiteScope for a Non-English Locale" on page 216.
- When deploying the Web Script Monitor, script names and transaction names must also be in English characters.

Multi-Lingual User (MLU) Interface Support

The SiteScope user interface can be viewed in the following languages in your Web browser:

Language	Language Preference in Web Browser
English	English
Simplified Chinese	Chinese (China) [zh-cn], Chinese (Singapore) [zh-sg]
Korean	Korean [ko]
Japanese	Japanese [ja]

Use the language preference option in your browser to select how to view SiteScope. The language preference chosen affects only the user's local machine and not the SiteScope machine or any other user accessing the same SiteScope. For details on setting the user interface viewing language, see "View SiteScope User Interface in a Specific Language" on page 217.

Note: The language is determined when you log in to SiteScope; changing the language preference in your browser once you have logged in has no affect until you log out and log back in.

Notes and Limitations

- There is no language pack installation. All translated languages are integrated into SiteScope Multi-lingual User interface (MLU).
- Data stays in the language it was entered in, even if the language of the Web browser changes. Changing the language of the Web browser on your local machine does not change the language of monitor definitions and configurations.
- SiteScope Help changes to the language that you have selected for the user interface. When you select **Help on this page** or **SiteScope Help**, it is displayed in the language you selected.

To activate this feature, you must install a software patch. Contact HP Customer Support for further information.

- Other links in the Help drop-down list, such as SiteScope Knowledge Base FAQ, Customer Support Web Site, and HP Software Web Site, are also displayed in the user interface language you selected.

Database Environment Issues

- When you create a new Oracle instance in an Oracle database, you must specify the character set for the instance. All character data, including data in the data dictionary, is stored in the instance's character set.
- The Database Query Monitor can connect to an Oracle database but the Oracle user names and passwords must contain only English characters.

Monitors Tested for Internationalization

The following monitors have been tested for internationalization.

Windows Operating System

- CPU Monitor
- Database Counter Monitor
- Database Query Monitor
- Disk Space Monitor
- IIS Server Monitor
- Link Check Monitor
- Log File Memory Monitor
- Oracle 10g Application Server Monitor
- Oracle 9i Application Server Monitor
- Ping Monitor
- Script Monitor
- Service Monitor
- SNMP Monitor
- SNMP Trap Monitor

- SQL Server Monitor
- UDDI Monitor
- URL Monitor
- URL Content Monitor
- URL List Monitor
- URL Sequence Monitor
- Web Script Monitor
- Windows Event Log Monitor
- Windows Performance Counter Monitor
- Windows Resources Monitor

UNIX Operating System

- CPU Monitor
- Database Query Monitor
- Disk Space Monitor
- Log File Monitor
- Port Monitor
- Script Monitor
- Service Monitor
- UNIX Resources Monitor
- URL Monitor
- URL Content Monitor
- URL Sequence Monitor

Using Default Authentication Credentials

You use this section to enter default authentication credentials that SiteScope uses to log into certain applications and systems. This user name and password are used if the following conditions are met:

- No other authentication credentials are entered as part of an individual monitor configuration.
- The target application or system requires authentication credentials.The following monitor types can use this feature:
  - URL Monitor
  - URL Sequence Monitor
  - Web Service Monitor

Complete the entries for default authentication as described in the Main Settings section in "SiteScope General Preferences" on page 226.

Suspending Monitor Processes

In large and complex monitoring environments, it is possible that SiteScope can become heavily loaded with a large number of monitors running and the responsiveness may become slow. This may be due to some monitors being configured to monitor too aggressively or systems that are becoming overloaded. If monitoring actions are slowing the performance of SiteScope, it can be useful to temporarily suspend monitoring actions to make configuration changes. You can temporarily suspend monitors to reduce the time required to complete large configuration operations such as a global search and replace operation. The **Suspend Monitors** option provides this function.

Working with SiteScope Configuration Files

SiteScope uses a binary monitor and system configuration data storage for the SiteScope application. This is different than versions of SiteScope earlier than 8.0.0.0 which stored monitor and system configuration data in text files in the **SiteScope\groups** directory.

This option is selected by default when SiteScope is installed. You should leave this option selected if you plan to make changes or additions to the **master.config** file or manually edit other files in the groups folder. If this option is not selected, SiteScope ignores changes made to the text configuration files.

Disabling this option may improve SiteScope performance.

Note: If you disable this option and later want to re-enable it, you must select the box, click **OK** to save the change, and then restart SiteScope to complete the change.

Web Script Monitor Files Directory

The Web Script Monitor runs VuGen scripts to monitor performance and content on Web applications. The VuGen scripts used by the monitor can be stored in the default directory for these scripts, **<SiteScope root directory>/templates.webscripts**, or you can define a different directory in General Preferences.

Note: The Web Script monitor is available only to users accessing SiteScope directly and not to users accessing SiteScope via System Availability Management Administration in HP Business Availability Center.

Configuring General Preferences

For details on configuring these preferences, see “SiteScope General Preferences” on page 226.

HP Business Availability Center Preferences Overview

This section includes the main concepts related to HP Business Availability Center Preferences.

Registering SiteScope to an HP Business Availability Center

To enable logging of SiteScope monitor data to Business Availability Center, the SiteScope must be configured as a data collector for Business Availability Center.

- On the SiteScope side, the Business Availability Center must be registered to the SiteScope in the BAC Preferences page.
- On the Business Availability Center side, add a SiteScope to the System Availability Management Administration page. For details, see "New SiteScope Page" on page 47.

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

Note: Monitors created in SiteScope before registration to Business Availability Center have their logging option set to **Do not report to HP Business Availability Center**. After you configure SiteScope as a data collector reporting to Business Availability Center, the default new monitors created in SiteScope is to log their monitoring data to Business Availability Center.

To change logging options use either the Business Availability Center logging options on the BAC Preferences page, or edit a specific monitor and select the **Do not report to HP Business Availability Center** option in the **HP BAC Logging** section of the edit monitor page. For details, see "HP Business Availability Center Preferences" on page 233 and "HP BAC Logging" on page 613.

Specifying Connection Parameters to HP Business Availability Center Servers

Complete the options as indicated in "HP Business Availability Center Preferences" on page 233.

Selecting the Profile

Select the SiteScope profile in which HP Business Availability Center stores the data collected by SiteScope (the SiteScope profile must have been previously added to System Availability Management Administration in Business Availability Center).

Note:

- Only SiteScope profiles not in use by any other SiteScope or HP Business Availability Center data collector appear in the list.
- When viewing reports in HP Business Availability Center, you select this profile to see the SiteScope data.
- It is recommended that you use the word **SiteScope** in the profile name to identify SiteScope profiles in HP Business Availability Center.

Using SSL for SiteScope-HP Business Availability Center Communication

You can use Secure Sockets Layer (SSL) to transmit data from SiteScope to the Business Availability Center server. If you have installed a certificate signed by a root Certificate Authority on the Business Availability Center server, no additional setup is required on the SiteScope server. If you are using a self-signed certificate on the HP Business Availability Center server and want to use that certificate for secure communication with SiteScope, you need to do the following:

- Add three entries to the **master.config** file on the SiteScope server as described below.
- Import the certificate from the Business Availability Center server to the keystore on the SiteScope server.

Note:

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

To enable secure communication between SiteScope and HP Business Availability Center using a self-signed certificate:

1 Obtain a copy of the self-signed certificate from the Business Availability Center server saved in a DER-encoded binary X.509 format. Normally, the certificate file has an extension of *.cer.

2 Import the certificate into a keystore on the SiteScope server using the procedures described in "Configuring SiteScope to Use SSL" in the *HP SiteScope Deployment Guide* PDF.

Note: It is not necessary to create the certificate request file, since you already have a certificate.

3 Edit the **master.config** file in the <**SiteScope_root_directory**>**groups** using a text editor. Add the following three entries with the data indicated:

```
_sslTrustedCertKeyStoreFile=<path>\<filename>
_sslTrustedCertKeyStorePassword=<keystorepassword>
_sslAcceptAllUntrustedCerts=<boolean>
```

For example, the entries added to the **master.config** file might be as follows:

```
_sslTrustedCertKeyStoreFile=c:\keystores\topaz.keystore
_sslTrustedCertKeyStorePassword=sUp3rS3cr3tP@ssw0RD
_sslAcceptAllUntrustedCerts=false
```

4 Save the changes to the file.

5 Restart the SiteScope server.

Changing the Gateway Server to Which SiteScope Sends Data

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

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

Troubleshooting Data Reporting to Business Availability Center

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

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

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

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

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

Configuring Business Availability Center Preferences

For details on configuring these preferences, see "HP Business Availability Center Preferences" on page 233.

Failover Preferences Overview

Note: The Failover Preferences are available only to users accessing SiteScope High Availability that have a SiteScope Failover License.

When using SiteScope Failover, a special version of SiteScope that includes automated mirroring and failover functionality, you can use Failover Preferences to indicate a primary SiteScope to be mirrored and set how often the configurations should be mirrored to the failover SiteScope installation.

For details on configuring these preferences, see “Failover Preferences” on page 236.

Infrastructure Settings Preferences Overview

SiteScope enables you to define the value of many settings that determine how SiteScope runs.

In the Infrastructure Settings Preferences, you can select different contexts from which to view and edit settings. These contexts are split into four groups:

- **General Settings.**

  This list includes those settings that determine the general infrastructure in SiteScope.

- **Server Settings.**

  This list includes those settings that determine the behavior of the SiteScope Server during start up, shut down, and while running.

- **Monitor Settings.**

  This list includes those settings that determine how different monitors within SiteScope behave.

- **Other Settings.**

  This list includes various other infrastructure properties.

For details on configuring these preferences, see “Infrastructure Settings Preferences” on page 238.

Windows Remote Preferences Overview

Monitoring resources at the server level can be done using a login connection to the remote server. SiteScope automates monitoring server resources on remote Windows servers by running tools that access data on the remote machine. To do this, SiteScope must be able to establish a connection to the servers you want to monitor. It must also be authenticated as a user having permissions to access the Windows performance registry on the remote machine.

For SiteScope running on Windows, there are two methods for enabling SiteScope to monitor data on remote Windows servers:

- Define an individual remote Windows server connection profile for each server.
- Set domain privileges to permit SiteScope to access remote servers.

After you define a Windows server connection profile or provide the necessary domain administration privileges, you need to configure user permissions for remote monitoring on the SiteScope machine and have SiteScope test the settings. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 218.

You can then create monitors to watch the resources and performance counters for that server. Multiple monitors can use the same connection profile. Click the **Servers** list on an New Monitor page to display a list of the remote servers you have defined. You can then select the server that you want to monitor.

Technical Notes on Remote Windows Monitoring

The following is additional information relating to the setup of and troubleshooting SiteScope monitoring of remote Windows NT and Windows 2000 servers.

A general troubleshooting step in working with remote Windows servers with SiteScope for Windows NT/2000 is to connect to the remote machine using PERFMON. If a connection cannot be made using this tool, there is likely a problem involving the user access permissions granted to the SiteScope account on the remote server. SiteScope requires certain administrative permissions to be able to monitor server statistics.

For security reasons, SiteScope may not be allowed to use the permissions of a full administrator account. SiteScope can be granted restricted monitoring access by editing certain Windows Registry Keys. For more information on restricting access to the registry from a remote machine, refer to the Microsoft Knowledge Base (http://support.microsoft.com/kb/q153183/).

When you need to monitor a server which is a stand-alone server or not part of a domain already visible to the SiteScope server, try entering the machine name followed by a slash and then the login name in the **Login** box. For example, loneserver\sitescope.

Some problems have been found when trying to monitor Windows 2000 servers from SiteScope running on Windows NT4. In many cases, the problem involves incompatibility of the DLL's used by the operating system to communicate between the servers.

Note:

- For additional information on how to secure performance data in Windows 2000, Windows NT, and Windows XP, refer to the Microsoft Knowledge Base (http://support.microsoft.com/kb/q146906/).
- For information on troubleshooting performance monitor counter problems for Windows 2000 and Windows NT, refer to the Microsoft Knowledge Base (http://support.microsoft.com/kb/152513/).

Troubleshooting Windows Event Log Access on Remote Windows Servers

Problem

When viewing Remote Windows event logs or getting alerts relating to monitoring a remote Windows machine, the following message is displayed:

```
The description for Event ID ( XXXX ) in Source ( XXXX ) could not be found. It contains
the following insertion string(s):
The operation has completed successfully.
```

Cause:

When you view the event log on a computer from a remote computer, if the required registry keys (and referenced files) are not present on the remote computer, SiteScope is unable to format the data; hence it displays the data in a generic format.

Resolution:

The required registry entries and DLL files must be copied to the remote computer on which the event viewer application is being run. Follow these steps to get the remote registry entries and DLL files onto the local SiteScope machine:

1. Locate on the remote machine which event you are not getting properly in SiteScope by finding the entry in the Event Viewer. Write down the information for the source, event id, and description. For example:

```
Source: MSExchangeSA, Event ID: 5008, Description: The message tracking log file
C:\exchsrvr\tracking.log\20020723.log was deleted.
```

2. Open the registry setting **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application** and click the source (for example, MSExchangeSA).
3. Click **EventMessageFile** and write down the data for where that DLL is located (for example, C:\EXCHSRVR\bin\madmsg.dll).

4. Locate the DLL on the remote and copy it to the SiteScope machine. You can perform the copy in one of two ways:

   - Use the **Initlog.exe** utility, in the BackOffice Resource Kit, Second Edition, to copy the required registry entries from the Exchange Server computer to the remote computer. This utility can also copy the required DLL files if you are logged on to Windows NT with an account that has Administrator privilege on the Exchange Server computer (see Microsoft Article Q184719).

   - Use FTP, mail, and so forth, to get the file to your local drive.

5. SiteScope uses the data from the **EventMessageFile** field in step 3 to determine where to find the DLL on the local machine. You must create the same folder structure as in this step and place the file in that directory. Alternatively, you can change the directory structure to say c:\Windows\System32 (SiteScope looks in the ADMIN$ by default on the remote machine), and place the DLL in that folder, but you must have this structure and the DLL on both machines. If you do this, you need to update the registry in step 3 to reflect the directory in which the DLL is located.

Using Perfex for Troubleshooting Remote Windows Connections

Use the following steps to view that data is being returned when SiteScope is trying to access the remote registry:

1. Open a command window on the SiteScope server.
2. Change directory to the <**SiteScope install path**>\SiteScope\tools directory.
3. Type the following in a command line:

```
perfex \\MACHINE -u username -p password -d -elast "Application"
```

This command gives you the number of entries in your Application log. For example:

```
Connected to \\ex-srv as int-ss Next Record: 2369
```

4 You should list only the last 10 or 12 events to find the one you are looking for. For this example, the command is:

```
perfex \\MACHINE -u username -p password -d -elog "Application" 2355 | more
```

5 Look through each entry until you find the one you need. Note the Record id for easier searching next time when using the command in Step 3.

6 This output tells you what data SiteScope is receiving. In the example given, the following is an example of the data that typically would be returned:

```
Type: Information
Time: 02:00:24 08/01/102
Source: MSExchangeMTA
ID: 298
Category: 1
Record: 2342
Machine: EX-SRV
FILE=C:\EXCHSRVR\res\mtamsg.dll
REMOTE FILE=
String 835050d is: MTA
Next String 835054d is: OPERATOR
Next String 83505dd is: 34
Next String 835060d is: 0
Next String 835062d is:
File: C:\EXCHSRVR\res\mtamsg.dll
Remote Path:
calling FormatMessage()
Formatted Message 142 bytes long
Raw message is: The most current routing information has been loaded by the MTA,
and a text copy was saved in the fileGWART0.MTA. [MTA OPERATOR 34 0] (12)
Message: The most current routing information has been loaded by the MTA, and a text
copy was saved in the file GWART0.MTA.[MTA OPERATOR 34 0] (12)
```

The file path is where the remote file is being found. If you copy the DLL to the WINDOWS\SYSTEM, the file and remote file path like this:

```
Type: Information
Time: 03:15:00 08/01/102
Source: MSExchangeIS Public
ID: 1221
Category: 6
Record: 2350
Machine: EX-SRV
FILE=C:\WINNT\SYSTEM32\mdbmsg.dll
REMOTE FILE=\\ex-srv\ADMIN$\SYSTEM32\mdbmsg.dll
String 835054d is: 0
Next String 835056d is:
File: C:\WINNT\SYSTEM32\mdbmsg.dll
Remote Path: \\ex-srv\ADMIN$\SYSTEM32\mdbmsg.dll
LOADING LIB REMOTE: \\ex-srv\ADMIN$\SYSTEM32\mdbmsg.dllcalling
FormatMessage()Formatted Message 89 bytes long
Raw message is: The database has 0 megabytes of free spaceafter online
defragmentation has terminated.Message: The database has 0 megabytes of free
space afteronline defragmentation has terminated.
```

Configuring Windows Remote Preferences

For details on configuring these preferences, see “Windows Remote Preferences” on page 239.

UNIX Remote Preferences Overview

Monitoring resources at the server level can be done using a login connection to the remote server. SiteScope automates monitoring of server resources on remote UNIX servers by running command line tools on the remote machine as a remote user. To do this, SiteScope must be able to establish a connection to the servers to be monitored and authenticated as a remote user with permissions to execute the applicable commands.

Before configuring SiteScope monitors to monitor resources on a remote UNIX server, you need to define a remote UNIX server connection profile for that server. You also need to create or modify an account on the remote server that corresponds with the connection method and permissions you intend to grant to SiteScope as a "remote user" logging onto that server.

After you define a remote UNIX connection profile, you can create monitors to watch the resources of that server. Multiple monitors can use the same connection profile. Clicking the **Servers** list on an New Monitor page displays a list of the remote servers you have defined. You can then select the server that you want to monitor.

Note: You can use SiteScope UNIX operating system adapters to extend SiteScope to connect to, and remotely monitor versions of UNIX that are not supported by default. For details, see “UNIX Operating System Adaptors” on page 1323.

Connection Methods for Remote UNIX

You can choose one of several methods that SiteScope should use to connect to remote UNIX servers. These include:

Connection Method	Description
telnet	Along with SSH, telnet is another popular method for connecting to remote UNIX servers. You can set up your remote servers to require a password for telnet, or to allow access without a password (like "rsh"). SiteScope handles either case.
SSH	For Solaris, using the SSH access method requires that an SSH client is installed on the SiteScope machine and the SSH server installed on the servers you are monitoring. See the document on Secure Shell in the Advanced SiteScope Topics section for more information on SSH requirements. The path to the SSH client on the machine where SiteScope is running should be **/usr/local/bin/ssh** or **/usr/bin/ssh**. For Windows NT or 2000, an SSH client is included in the package. For debugging, the Windows SSH client can be run from the command line, replacing the values for the username, host name, and password: `\SiteScope\tools\plink.exe -ssh myUser@myServer.myCompany.com -pw myPassword` Using SSH requires that digital certificates be installed on each of the servers to which you are connecting.

Connection Method	Description
rlogin	You can set up your remote servers to require a password for rlogin, or to allow access without a password (like "rsh"). SiteScope supports either case.
HTTP	There are some cases where it may be useful to use a Common Gateway Interface program over HTTP to access performance data or application data from a UNIX server. Two simple CGI scripts are included with SiteScope to allow access over HTTP: ➤ **<SiteScope root directory>/conf/examples/remote.pl** ➤ **<SiteScope root directory>/conf/examples/remote.sh** The **remote.pl** CGI is a Perl (version 4 and above) script that executes a command on the server; the **remote.sh** script does the same, except as a UNIX sh script. CGI commands are passed in using the COMMAND CGI variable. If you are using the CGI connection method and you want to use remote actions, remember that the permissions for both the directory containing the CGI script and the **/script** directory need to allow the Web server (probably running as a user with few permissions) to execute in those directories. Additionally, the scripts need to have execute permission. If you want to use a CGI script that puts more restrictive limits on the commands that can be run, you can use a different CGI script. All that matters is that the CGI returns the output of the command passed in using the COMMAND variable. For greater security, it is recommended to set up your Web server to require a login/password authorization to run the script. Also, if you have a secure Web server on that server, you can set up the script to run using the Secure Sockets Layer (SSL used in HTTPS requests), so that the request and output is encrypted.

Configuring UNIX Remote Preferences

For details on configuring these preferences, see “UNIX Remote Preferences” on page 243.

Log Preferences Overview

Log Preferences enable you to select how much monitor data is accumulated and maintained on the SiteScope server. It also configures SiteScope to export monitor data to an external database.

By default, SiteScope saves monitor results, alert data, error data, and other readings returned by monitors into log files. For monitor data results, a date-coded log file is created for each 24-hour period of monitoring. This data is stored as tab delimited text. SiteScope uses the log files to generate management reports on system availability and performance over time.

Since storing data logs can become a problem over time, you can limit how much log information SiteScope saves to the local file system. The amount of data can be limited to the number of days to maintain log files or to a maximum data log file size. You can also send monitoring data to an external database application. This helps reduce the data storage capacity required on the SiteScope server and makes the monitoring data available to other reporting tools.

Note: To create SiteScope Management Reports the monitoring log information for the desired time period of the report must be available on the SiteScope server file system.

Troubleshooting Database Connections

When Database logging is active and working correctly, you should see a table called **SiteScopeLog** in your database and a record added to the table every time a monitor runs. The data is sent to the database as a single table in a flat-file format.

If the **SiteScopeLog** table is not created or is empty, check the SiteScope **<SiteScope install path>/SiteScope/logs/RunMonitor.log** and **<SiteScope install path>/SiteScope/logs/Error.log** files for log messages starting with "jdbc" or "odbc". When Database logging is working correctly, you should see a set of messages in **RunMonitor.log** that looks like this:

```
jdbc log, reconnect seconds=600
jdbc log, loading, driver=sun.jdbc.odbc.JdbcOdbcDriver
jdbc log, connecting, url=jdbc:odbc:SiteScopeLog,
jdbc log, logged in
jdbc log, checking log table
jdbc log, created log table
jdbc log, prepare insert, 19, INSERT INTO SiteScopeLog...
jdbc log, connected
```

If these entries do not appear in the log file there is a problem with the database interface or configuration of the database connection. You should also check the Database Connection URL you entered. This parameter is case sensitive. Check the spelling and letter case of the connection URL and be sure there are no leading or trailing spaces present in the text box.

You can also check the online Knowledge Base available via the Customer Support site for other information relating to database logging.

SiteScope Log Database Table Structure

When database login is enabled, monitor data is contained in a single table called **SiteScopeLog**. The first nine fields of each database record are the same for all monitors. The next ten fields contain different measurements depending on the kind of monitor supplying the data. All the fields in the table use the VARCHAR(255) data type. A description of the fields in the log database record are shown in the table below along with their default field names:

Field Name	Example Data	Description
datex	1999-01-20 11:54:54	The first field contains the date that the monitor ran.
serverName	demo.sitescope.com	The second field contains the name of the server where SiteScope is running.
class	URLMonitor	The third field contains the type of the monitor.
sample	23	The fourth field contains the sample number of this monitor.
category	good	The fifth field contains the category name of the monitor.
groupName	URLs	The sixth field contains the group name of the monitor.
monitorName	Home Page	The seventh field contains the name of the monitor.
status	1.01 seconds	The eighth field contains the status of the monitor.
monitorID	10	The ninth field contains the ID of the monitor.
value1, value2, ... value10	(variable)	The tenth through nineteenth fields contain the monitor specific data as described in the Log Columns page. The first variable field (value1) corresponds to the value listed as column 7 in the log files.

The SQL statement that is used for database logging can be changed by editing the parameter _logJdbcInsertSiteScopeLog= in the **SiteScope/groups/master.config** file. A stored procedure can be called by replacing the insert statement with a call statement. For example, call logit(?,?,?) would call the stored procedure named logit passing it the first three parameters.

Configuring Log Preferences

For details on configuring these preferences, see "Log Preferences" on page 250.

E-mail Preferences Overview

The E-mail Preferences container includes two view panels; the Properties panel and the Contents panel.

- **E-mail Preferences Properties panel.** Use to configure the settings SiteScope needs to communicate with an external e-mail server. These are the default settings that SiteScope uses to send alerts as e-mail messages.
- **E-mail Preferences Contents panel.** Use to define custom E-Mail Recipient profiles to send e-mail alert messages to recipients other than the one defined in the Properties panel. The E-mail Recipient profile can then be associated with one or more E-mail alerts by editing the applicable alert definition.

For details on configuring these preferences, see "E-mail Preferences" on page 252.

Pager Preferences Overview

Pager Preferences includes two view panels; the Properties panel and the Contents panel.

- **Pager Preferences Properties panel.** Use to configure the settings SiteScope needs to communicate with an external electronic paging service. These are the default settings that SiteScope uses to send alerts to an electronic pager.
- **Pager Preferences Contents panel.** Use to define custom Pager Recipient profiles other than the one defined in the Properties panel. The Pager Recipient profile can then be associate with one or more Pager alerts by editing the applicable alert definition.

Pager Connection Options

The preferred pager connection option is to connect directly to a **modem at your pager service**. When a modem-to-modem connection is used, SiteScope is able to verify that the message was sent successfully and can receive messages describing any communication problem. The other connection options generally send messages to automated voice response systems using touch tone dialing. The touch tone dialing method is limited to numeric messages and SiteScope cannot confirm that your paging service correctly received the message.

Modem Numbers

If you have an alphanumeric pager and use an alphanumeric paging service, you must enter the phone number to use for sending alphanumeric pages to the paging service modem. This number is provided by your paging service. Sometimes, the paging service calls this the TAP/IXO number.

Configuring Pager Preferences

For details on configuring these preferences, see “Pager Preferences” on page 257.

SNMP Trap Preferences Overview

The SNMP Trap Preferences container includes two view panels; the Properties panel and the Contents panel.

- **SNMP Trap Preferences Properties panel.** Use to configure the settings SiteScope needs to communicate with an external SNMP host or management console. These are the default SNMP parameters for use with SNMP Trap alerts.
- **SNMP Trap Preferences Contents panel.** Use to define custom SNMP Trap profiles or templates to send traps to hosts other than the one defined in the Properties panel. The SNMP Trap profile can then be associated with one or more SNMP Trap alerts by editing the applicable alert definition.

For details on configuring these preferences, see “SNMP Trap Preferences” on page 262.

Dynamic Update Preferences Overview

Note: The Dynamic Update Preferences are available only to users accessing SiteScope directly and not to users accessing SiteScope via System Availability Management Administration in HP Business Availability Center.

Dynamic Update automatically creates and deploys SiteScope server availability monitoring based on information in an external data source. SiteScope can regularly query this data source for new IP addresses to monitor. SiteScope can query a SNMP Management Information Base (MIB) or, alternatively, a database, and then automatically create a set of server availability monitors for each new IP address that is found. A Dynamic Update set can query either a SNMP MIB or a database, but not both. Use the Dynamic Update feature to rapidly deploy SiteScope monitoring when deploying SiteScope for the first time in a network or data center.

You enable this feature by creating one or more Dynamic Update sets and specifying an update frequency. SiteScope automatically creates monitors based on the associated template whenever it detects new records in the target data source. The Dynamic Update set remains active until deleted from the Dynamic Update Set table. You can create multiple Dynamic Update sets using different data sources, monitor set templates, and update settings.

For details on configuring these preferences, see “Dynamic Update Preferences” on page 264.

Absolute Schedule Preferences Overview

SiteScope monitors, alerts, and reports are enabled 24 hours a day, 7 days a week, 365 days a year by default. This means that as long as a monitor is enabled, it is run according to the update frequency specified in the individual monitor configuration. For example, if a monitor is configured to run every 30 seconds, SiteScope attempts to run the monitor every 30 seconds throughout the day. If SiteScope detects an error condition, any associated alert is executed as well, regardless of the time of day.

In some situations, it is useful to enable certain SiteScope actions to correspond with a single event or a particular time of day. For example, you may want to use this type of scheduling for monitors, such as the Link Checking monitor, which you want to run only once a day at a time when the server generally has a lighter load.

Absolute Scheduling lets you set specific times that a monitor is run on a weekly basis. Absolute schedules are reset at the end of the week and repeated each week. Absolute Schedule Preferences triggers a monitor to run only once at each time specified in the schedule.

Absolute Schedule Preferences are inactive until they are explicitly associated with a monitor instance. Use the Advanced Settings section of a monitor configuration page to associate Absolute Schedule Preferences with a monitor.

Note: Absolute Schedule Preferences are associated to alerts indirectly by way of the monitors associated with the alert. Any alerts associated with the monitors disabled by Absolute Schedule Preferences are effectively disabled for the period during which those monitors are disabled. However, if an alert is associated with other monitors that are not controlled by the same schedule, that alert is still triggered if the other monitors report an error condition.

For details on configuring these preferences, see "Absolute Schedule Preferences" on page 268.

Range Schedule Preferences Overview

SiteScope monitors, alerts, and reports are enabled 24 hours a day, 7 days a week, 365 days a year by default. This means that as long as a monitor is enabled, it is run according to the update frequency specified in the individual monitor configuration. For example, if a monitor is configured to run every 30 seconds, SiteScope attempts to run the monitor every 30 seconds throughout the day. If SiteScope detects an error condition, any alert associated with the monitor is executed as well, regardless of the time of day.

In some situations, it is useful to enable and disable certain SiteScope actions based on the schedules of the individuals or groups responsible for the servers and systems being monitored. You use Range Schedule Preferences to instruct SiteScope to enable or disable monitors according to time periods that you define.

You can use Range Scheduling to specify a time range during which SiteScope either enables or disables particular monitors. If you specify an enabled time range for a new monitor (using the Advanced Options on the Add monitor page), SiteScope only runs the monitor during that range. For example, if you create a range of 8AM- 9PM, Monday through Friday, any monitors that have that range schedule associated with them are run only during those times.

A common use of range scheduling is to set up different pager alerts associated with monitors running at times that coincide with work shifts when different administrators are on call. The schedule helps prevent pager alerts being sent to individuals at an inappropriate time of day relative to the work schedule of that individual.

Range Schedule Preferences are inactive until they are explicitly associated with a monitor instance. You use the Advanced Settings section of a monitor configuration page to associate Range Schedule Preferences with a monitor.

Note: Range Schedule Preference are associated to alerts indirectly by way of the monitors associated with the alert. Any alerts associated with the monitors disabled by Range Schedule Preference are effectively disabled for the period during which those monitors are disabled. However, if an alert is associated with other monitors that are not controlled by the same schedule, that alert is still triggered if the other monitors report an error condition.

For details on configuring these preferences, see "Range Schedule Preferences" on page 270.

User Preferences Overview

Note: The User Preferences are available only to users accessing SiteScope directly and not to users accessing SiteScope via System Availability Management Administration in HP Business Availability Center.

You manage SiteScope user accounts from the Users Preferences page. This page enables you to administer the users that are allowed access to SiteScope.

As a client-server based architecture, a single SiteScope user profile can be accessed by multiple users simultaneously. You can define multiple SiteScope user accounts that provide different view and edit permissions for different audiences. For example, you can create a user profile that allows users to view monitor status and reports but does not allow the users to add or edit monitor configurations or alerts.

A user profile limits access to SiteScope to those users that enter a correct user name and password. Optionally, user authentication can be handled by submitting a query to a LDAP database. For more restrictive access control to SiteScope, see "SiteScope General Preferences" on page 226 for options on how to restrict access to SiteScope to certain IP addresses only.

A user profile has two main components:

- User authentication information and access permission
- Action permissions

Configure these settings for each user profile in the applicable User Profile container.

For details on changing a user password, see “Change a User’s Password” on page 222.

User Types

SiteScope provides the following user types:

- **Administrator.** SiteScope provides a single administrator by default. An administrator can view and change anything in SiteScope. It has other special properties as well, such as being allowed to create other users and to change their profiles on the Users Preferences form. The administrator account cannot be disabled or deleted.
- **Power user (super user).** A power user has all the permissions of an administrator except that it cannot delete itself or the administrator. Both an administrator and a power user can create a power user. There may exist any number of power users. For details about enabling this user type, see “Preference Settings” on page 276.
- **Regular User.** A regular user cannot create, delete, or edit other users. It has all the permissions defined for it by the administrator or power user.

Note:

- The administrator account is the default account used when accessing SiteScope. This means that anyone requesting the server address and port number where SiteScope is running is, by default, logged in on the administrator account. To restrict access to this account and its privileges, you need to edit the administrator account profile to include a user login name and login password. SiteScope then displays a login dialog before SiteScope can be accessed.
- You can create a named user account that does not require a user login name and password. You do this by creating a new user profile by providing a **Title**, but leaving the **Login Name** and **Password** fields blank. With this configuration, users accessing SiteScope are presented with an authentication dialogue. They may be authenticated as this named user by leaving the **Login Name** and **Password** fields blank and clicking the **Log In** button.
- You should restrict the permissions on this type of account to avoid unauthorized changes to your SiteScope configuration.

Configuring User Preferences

For details on configuring these preferences, see “User Preferences” on page 272.

Configure SiteScope for a Non-English Locale

Perform the following steps to configure SiteScope for a non-English locale, and override the default locale date and time settings used by SiteScope.

To configure SiteScope for a non-English locale:

1. In the left menu tree, expand **Preferences** and click **General Preferences**. The General Preferences page opens.
2. Click **Edit.** The Main Settings view opens.
3. Select **International Version**.
4. Click **OK**.
5. Restart SiteScope.

To set new locale data and time settings to be used by SiteScope:

1. Edit the master.config file in the **<SiteScope install path>/SiteScope/groups** directory.
2. Find the entry "_localeCountry=", and assign it an uppercase 2-character ISO-3166 country code. A full list of these codes is at a number of sites, such as http://www.chemie.fu-berlin.de/diverse/doc/ISO_3166.html. For example:
   _localeCountry=US
3. Find the entry "_localeLanguage=", and assign it a lowercase 2-character ISO-639 language code. A full list of these codes is at a number of sites, such as http://www.ics.uci.edu/pub/ietf/http/related/iso639.txt. For example:
   _localeLanguage=en
4. Save the **master.config** file.
5. Restart SiteScope.

View SiteScope User Interface in a Specific Language

You can select a language preference for viewing the SiteScope user interface. See "Multi-Lingual User (MLU) Interface Support" on page 183 for a list of supported languages.

To view SiteScope user interface in a specific language:

1. Install the appropriate language's fonts on your local machine if they have not yet been installed. If you choose a language in your Web browser whose fonts have not been installed, the SiteScope user interface uses the default language of your local machine.

   For example, the default language on your local machine is English and the Web browser is configured to use Japanese. If Japanese fonts are not installed on the local machine, the SiteScope user interface is displayed in English.

2. If you use Internet Explorer, configure the Web browser on your local machine to select the language in which you want to view the SiteScope user interface. For details, see http://support.microsoft.com/kb/306872/en-us. Go to step 4.

3. If you use FireFox, configure the Web browser on your local machine as follows:

   a. Select **Tools** > **Options** > **Advanced**. Click **Edit Languages**. The Language dialog box opens.

   b. Highlight the language in which you want to view SiteScope.

      If the language you want is not listed in the dialog box, expand the **Select language to add...** list, select the language, and click **Add**.

   c. Click **Move Up** to move the selected language to the first row.

   d. Click **OK** to save the settings. Click **OK** to close the Language dialog box.

4. Click **LOGOUT** at the top of the SiteScope window. SiteScope immediately refreshes and the user interface is displayed in the selected language.

Configure SiteScope to Monitor a Remote Windows Server

You can enable SiteScope to monitor data on remote Windows servers either by:

- Defining an individual remote Windows server connection profile for each server.
- Setting domain privileges to permit SiteScope to access remote servers.

After you define a Windows server connection profile or provide the necessary domain administration privileges, configure user permissions on the SiteScope machine to ensure that SiteScope has permissions to access the remote machine and test the connection settings.

This section includes the following topics:

- “Define Remote Windows Server Connection Profiles” on page 218
- “Set Domain Privileges for SiteScope Monitoring” on page 219
- “Configure User Permissions for Remote Monitoring” on page 220
- “Configure and Test the Settings for the Applicable Windows Remote Server” on page 222

Define Remote Windows Server Connection Profiles

Monitoring remote Windows server data requires authenticated access to the remote server. A Windows server connection profile provides the necessary address and login credentials for SiteScope to log in to a remote server and to access the Windows performance registry on that remote machine. To use this method, either:

- Log on to the remote server as a user with administrator privileges.
- Create or modify a user account on the remote server that corresponds with the connection method and login permissions used in the SiteScope connection profile for that server,

Set Domain Privileges for SiteScope Monitoring

SiteScope for Windows automatically generates a list of servers visible in the local domain. These servers are listed in the Servers list for monitor types where a server must be specified. SiteScope running on Windows may be able to use this list to monitor remote Windows servers without having to create individual connection profiles for each server.

You can set domain privileges using any of the following methods:

➤ **Set the SiteScope service to run as a user in the Domain Admin group.**

By default, SiteScope is installed to run as a Local System account. You can set the SiteScope service to log on as a user with domain administration privileges. This gives SiteScope access privileges to monitor server data within the domain.

➤ **Add the server where SiteScope is running to the Domain Admin group in ActiveDirectory (for Windows 2000 or later).**

With this option, the SiteScope service is set to log on as a Local System account, but the machine where SiteScope is running is added to a group having domain administration privileges.

➤ **Edit the registry access permissions for all machines in the domain to allow non-admin access.**

This option requires changes to the registry on each remote machine that you want to monitor. This means that while the list of servers in the domain includes all machines in the domain, only those remote machines whose registry has been modified can be monitored without use of a connection profile.

Configure User Permissions for Remote Monitoring

For SiteScope to collect performance measurements on a remote machine, SiteScope must have permission to access the remote machine. The procedure to configure user permissions varies according to the operating system on the SiteScope machine.

Note:

- Microsoft Best Practice recommends giving permissions to groups instead of to users.
- Back up the registry before making any registry changes.

To configure Windows XP and Windows 2003:

1. On the SiteScope machine, select **Start** > **Run**. In the Open text box, enter **Regedt32.exe**. The Registry Editor dialog box opens.
2. In the **HKEY_LOCAL_MACHINE** window, select **SOFTWARE** > **Microsoft** > **Windows NT** > **CurrentVersion** > **Perflib**.
3. Click **Security** in the Registry Editor tool bar and select **Permissions**. The Permissions for Perflib dialog box opens.
4. In the Name pane, highlight the user SiteScope uses to access the remote machine. In the Permissions pane, select the **Allow** check box for **Read**. Click **OK** to save the configuration and close the Permissions for Perflib dialog box.
5. In the **HKEY_LOCAL_MACHINE** window, select **SYSTEM** > **CurrentControlSet** > **Control** > **SecurePipeServers** > **winreg**. Click **Security** in the Registry Editor tool bar and select **Permissions**. The Permissions for Winreg dialog box opens.

6. In the Name pane, highlight the user that SiteScope uses to access the remote machine. In the Permissions pane, select the **Allow** check box for **Read**. Click **OK** to save the configuration and close the Permissions for Perflib dialog box.
7. In the Registry Editor tool bar, click **Registry** and select **Exit** to save the configuration and exit.
8. Restart the SiteScope machine.

Note: For more information on enabling non-administrative users to monitor performance on a remote machine, refer to the Microsoft Knowledge Base (http://support.microsoft.com/kb/q164018/).

To configure Windows 2000:

1. On the SiteScope machine, select **Start** > **Programs** > **Administrative Tools** > **Computer Management**. The Computer Management dialog box opens.
2. In the System Tools tree, expand the **Local Users and Groups** tree and select **Groups**. All groups on the machine are listed in the right-hand pane.
3. In the right-hand pane, select the **Administrators** group. The Administrators Properties dialog box opens.
4. If the user that SiteScope uses to access the remote machine is listed in the Members pane, go to step 5. If the user is not listed, click **Add**. The Select Users or Groups dialog box opens.
   a. Enter the user in the text box.
   b. Click **OK** to save the configuration and close the Select Users or Groups dialog box.
5. Click **OK** to save the configuration and close the Administrators Properties dialog box.
6. In the Computer Management dialog box, click **File** in the tool bar and select **Exit**.
7. Restart SiteScope on the SiteScope machine.

Configure and Test the Settings for the Applicable Windows Remote Server

Configure the remote Windows server in Windows Remote Preferences. For details, see "Windows Remote Preferences" on page 239.

After defining the Windows Remote Preferences definition for SiteScope, you can have SiteScope test the settings by clicking the **Test** link for the applicable server in the list of Windows Remote Preferences servers.

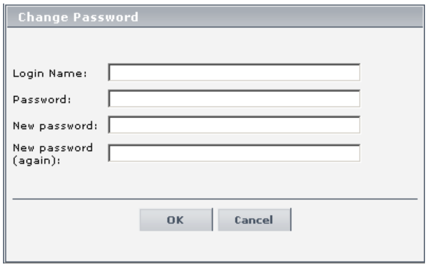
Note: If an unable to connect to remote machine error message opens when trying to view remote counters, refer to the Microsoft Knowledge Base (http://support.microsoft.com/kb/300702/).

Change a User's Password

To change a user's password, you must know the user's user name and current password.

To change a user's password:

1 In the SiteScope Login window, click the **Change Password** link in the lower-left part of the window. The Change Password dialog box opens.



2 Enter the user name, current password, and new password into the text boxes. Enter the new password a second time to confirm the entry.

3 Click **OK** to save your change and exit, or click **Cancel** to cancel your changes and exit.

If the new password does not comply with password configuration rules (see below for details), an error message is displayed and the password is not changed.

To configure password requirements:

You can configure password requirements by setting the following parameters in <**SiteScope root directory**>**groups****master.config**:

Parameter	Description
_adminMinimumLength = x	The password length must be at least **x** characters.
_adminRequireAlpha = (1,0)	➤ **0.** Password does not require an alphabetic character. ➤ **1.** Password must contain an alphabetic character.
_adminRequireNumber = (1,0)	➤ **0.** Password does not require a numeric character. ➤ **1.** Password must contain a numeric character.
_adminRequirePunctuation = (1,0)	➤ **0.** Password does not require punctuation. ➤ **1.** Password must contain punctuation.

14

Preferences User Interface Settings

This chapter includes the pages and dialog boxes that are part of the SiteScope Preferences user interface

SiteScope General Preferences

Description	Use to enter and view licensing information, and other general display features, optional features, and access options for SiteScope. **To access:** Expand **Preferences** in the monitor tree and click **General Preferences**.
Useful Links	"SiteScope General Preferences Overview" on page 182

The SiteScope General Preferences includes the following elements:

Main Settings

GUI Element	Description
License Number	Enter SiteScope license number to register SiteScope monitors. This number is issued when purchasing a set of monitors. A license must be purchased if intending to use SiteScope beyond the trial period.
Option Licenses	If you have purchased licensing for optional SiteScope monitoring capabilities, enter the license number. Generally, this license key has the same syntax as the SiteScope license. If you have purchased multiple license keys, enter each key separated with a comma.
Options Enabled	Displays information about the license as entered in the **License Number** and **Option Licenses** fields. This includes the total number of monitor points permitted by the license and how many points have been used, plus a label for any optional monitor license keys entered.
Locale-Specific Date and Time	Select to have SiteScope display dates and times in a format that is applicable to a certain locale, country, or culture. To use a different locale setting, modify the SiteScope configuration file to include the codes for the desired locale and select this option in the General Preferences Settings. **Default value:** United States format

GUI Element	Description
International Version	Select to enable international character sets. When this option is selected, SiteScope honors all character encoding. Use this option to instruct SiteScope to simultaneously handle character encoding from multiple sources and operating systems (for example, foreign language Web pages). If not selected, only the default character set of the operation system where SiteScope is installed is supported. The exceptions are all the URL monitor types, the Log File Monitor, and the File Monitor. These monitor types support multiple character encoding regardless of the International Version option setting.
Number of backups per file	Enter the number of SiteScope configuration file backups to be kept. This feature helps preserve important monitor, alert, and general SiteScope configuration information. This number represents the number of backups per file that is maintained. SiteScope uses a naming convention of filename.bak.1, filename.bak.2, filename.bak.#, where 1 is the latest backup file. **Example:** You can backup files containing general SiteScope configuration information in the <**SiteScope install path**>/**SiteScope/groups** directory.
Default Authentication Username	Enter the default user name to be used for authentication with remote systems. Both <username> and <DOMAIN>\<username> are valid formats. SiteScope uses this user name unless a different user name is entered explicitly as part of the monitor configuration.
Default Authentication Password	Enter the default password to be used for authentication with remote systems. SiteScope uses this password for the monitor types listed above unless a different password is entered explicitly as part of the monitor configuration.

GUI Element	Description
Preemptive Authorization	Select an option used for authenticating the default user credentials when SiteScope requests the target URL. ➤ **Authenticate first request.** Sends the username and password on the first request SiteScope makes for the target server. ➤ **Authenticate if requested.** Sends the username and password on the second request if the server requests a username and password.
Suspend All Monitors	Select to temporarily suspend the execution of all monitors. Use to make configuration changes across your monitoring infrastructure. To reactivate monitoring, clear the option. **Note:** This option disables all monitors currently defined for this SiteScope installation. If setting Suspend Monitors and later clearing this option to re-enable the monitors, the individual monitors that were set as disabled prior to the Suspend Monitors action, retain their original disabled state. Using this option may impact reports. Monitors that would have run during the time that monitoring was suspended may display blanks for that period in reports. **Warning:** There is currently no visual indication in the interface that SiteScope is in a suspended monitor state. When the **Suspend Monitors** option is enabled, the following message is displayed: SiteScope is in Suspended mode; no monitors are currently running.

GUI Element	Description
Enable Configuration Files	This option enables the use of the master and monitor group configuration files for SiteScope. When enabled, SiteScope periodically checks for changes to any files in the **SiteScope\groups** directory and updates the binary configuration data accordingly.
VuGen Scripts Path Route	Enter a directory to store the zip files of VuGen scripts for use by the Web Script Monitor. The files in the directory you enter here appear in the list of available scripts when configuring the Web Script Monitor. If you do not enter a value here, the files in the default directory <**SiteScope root directory**>**/templates.webscripts** appear when configuring the monitor. For details on working with the monitor, see "Web Script Monitor Overview" on page 589.

SSH Preferences

Description	Use to configure preferences for securely accessing a remote computer. **To access:** Expand **Preferences** in the monitor tree and click **General Preferences**. Click **SSH Preferences**.
Useful Links	"SiteScope General Preferences Overview" on page 182

The SSH Preferences includes the following elements:

GUI Element	Description
SSH V2 Connect Timeout	Enter the total number of seconds SiteScope should wait for a successful reply. When the time is exceeded, the connection is automatically closed. **Default value:** 30 seconds
SSH V2 Hello Timeout	Enter the handshake timeout (in seconds). **Default value:** 30 seconds
SSH V2 Key Exchange Timeout	Enter the total number of seconds SiteScope should wait for SSH key exchange. **Default value:** 30 seconds
SSH V2 Authentication Phase Timeout	Enter the total number of seconds SiteScope should wait for SSH authentication. **Default value:** 60 seconds
SSH Open Connections Limit	Enter the number of open SSH connections that SiteScope allows. If there are many monitors configured to use this connection, set the number of open connections high enough to relieve a potential bottleneck. **Note:** This setting does not effect running tests for a remote server. Tests always create a new connection. **Default value:** 500

Dashboard Monitor History View Options

Description	You configure Monitor History to view monitor history on all monitors and monitor groups. **To access:** Expand **Preferences** in the monitor tree and click **General Preferences**. Click **Dashboard Monitor History View Options**.
Important Information	In the Dashboard layout, you can then use a filter to further limit the monitors displayed to those that meet selected criteria. Your preferences are saved with the Dashboard filter settings. For details, see "Overview of Dashboard Filter" on page 336.
Useful Links	"Customize SiteScope Dashboard" on page 341

The Dashboard Monitor History View includes the following elements:

GUI Element	Description
Enable Monitor History View	Select to enable or disable Monitor History. **Default:** Disabled
Display Time Period	Select the time frame for displaying past runs.
Monitor Run Status	Select the appropriate run status.
Maximum Number of Runs to Display	Enter the number of rows of data to keep in memory.

JDBC Global Options

Description	Use to apply global JDBC options to the following resources that connect to the database: ➤ SiteScope database logger ➤ Database tools (Database Connection, Database Information) ➤ Database alerts ➤ Database monitors (Oracle database, Database Counter, Database Query, DB2 8.x, Technology Database Integration) **To access:** Expand **Preferences** in the monitor tree and click **General Preferences**. Click **JDBC Global Options**.
Useful Links	"SiteScope General Preferences Overview" on page 182

The JDBC Global Options includes the following elements:

GUI Element	Description
Connection Timeout	The amount of time, in seconds/minutes/hours/days, to wait for a new SQL connection to be made. Not all SQL drivers have this feature. If your SQL driver does not support this feature, this parameter is ignored. **Default value:** 1 minute
Driver Trace Log File	Used to create a driver trace log file for troubleshooting database drivers. This box is empty by default, and it is recommended that you use it only for troubleshooting. To create the log file, enter the full path or UNC name of the driver trace file (for example, e:\mydir\myfile.log). Note that the target log file might contain login information, table names and queries.

HP Business Availability Center Preferences

Description	Use to configure SiteScope as a data collector for Business Availability Center. **To access:** Expand **Preferences** in the monitor tree and click **BAC Preferences**.
Useful Links	"HP Business Availability Center Preferences Overview" on page 188

The Business Availability Center Preferences includes the following elements:

Main Settings

GUI Element	Description
Business Availability Center machine name/IP address	Enter the machine name or IP address of the Business Availability Center server to which you want this SiteScope to connect. **Note:** This is a required field.
SiteScope agent machine location	Enter the location of the SiteScope server that you are connecting to Business Availability Center. You can specify any value that helps you identify the location of this specific SiteScope server. **Note:** This is a required field.
Business Availability Center user name	Enter the username of a Business Availability Center administrator-level user.
Business Availability Center user password	Enter the password for the specified user.
Disable all logging to Business Availability Center	Select to stop SiteScope from sending data to Business Availability Center. Clear the check box to enable logging again.

Web Server Security Settings

GUI Element	Description
Authentication username	If the Business Availability Center server is configured to use basic authentication, enter the username to access the server.
Authentication password	If the Business Availability Center server is configured to use basic authentication, enter the password to access the server.
Use SSL (HTTPS protocol)	Select this option if the Business Availability Center server is configured to use the HTTPS protocol.

Proxy Server Settings

GUI Element	Description
Address	Enter the proxy server address if applicable.
Username	Enter the username for the proxy server.
Password	Enter the password for the specified server.

Topology Reporting Settings

GUI Element	Description
Enable host topology reporting	Select to enable Business Availability Center to automatically populate the CMDB with CIs based on the monitored hosts in SiteScope. If enabled, all the data necessary for creating a CI based on monitored hosts, including DNS name, is forwarded to Business Availability Center from the SiteScope. SiteScope forwards the host typology data: ➤ When a new monitor is created. ➤ When a monitor is edited. ➤ When SiteScope is restarted.

BAC Preferences Available Operations

GUI Element	Description
Re-synchronize	Force SiteScope to resend all its configuration data to Business Availability Center. This data consists of all the group and monitor definitions.
Hard Re-synchronize	Force SiteScope to resend all its configuration data to Business Availability Center and deletes the existing monitor and group data in Business Availability Center for this SiteScope.
Reset	This deletes all the UCMDB-related settings from the SiteScope server. This also sends a message to the applicable Business Availability Center server to release the SiteScope agent from the corresponding profile. **Note:** If you choose to reset the current settings, you have to create or use a different profile to reconnect SiteScope with Business Availability Center. Business Availability Center does not allow you to select a previously used connection profile.

Failover Preferences

Description	SiteScope Failover is a special version of SiteScope that includes automated mirroring and failover functionality. It enables you to implement failover capability for infrastructure monitoring by provisioning for backups, redundant, and failover mechanisms. Use the Failover Preferences to indicate a primary SiteScope to be mirrored and set how often the configurations should be mirrored to the failover SiteScope installation. **To access:** Expand **Preferences** in the monitor tree and click **Failover Preferences**.
Important Information	➤ The Failover Preferences are available only to users accessing SiteScope High Availability that have a SiteScope Failover License. ➤ SiteScope Failover restarts itself after each mirroring operation.
Useful Links	"Failover Preferences Overview" on page 194

The Failover Preferences includes the following elements:

Main Settings

GUI Element	Description
Host	Enter the name or IP address of the server that you want this SiteScope Failover server to mirror configurations from.
Port	Enter the SiteScope port of the server that you want this SiteScope Failover server to mirror configurations from (for example, 8888).
Use SSL	When this box is checked, the mirror server contacts the primary SiteScope server via HTTPS.
Admin login	The login name used to access the administrator login account for the primary SiteScope instance. If no administrator login has been configured on the target machine, leave this box blank.

GUI Element	Description
Admin password	The password used to access the administrator login account for the primary SiteScope instance. If no SiteScope administrator login has been configured on the primary SiteScope, leave this box blank.
Mirror every (hours)	The schedule for synchronizing (mirroring) configuration data to the failover SiteScope from the primary SiteScope. This is used to make sure that the SiteScope Failover configuration reflects updates and changes to the monitoring configuration on the primary SiteScope server. Values for this box should be between 1 to 23 hours. Enter values as whole numbers. **Default value:** 4 hours
Last mirror time	The time and date of the most recent mirroring operation.
Next scheduled mirror time	The time and date of the next scheduled mirroring operation.
Mirror Configuration Now	Click to mirror the primary SiteScope configuration data now.

Infrastructure Settings Preferences

Description	Enables you to define the values of many settings that determine how SiteScope runs. **To access:** Expand **Preferences** in the monitor tree and click **Infrastructure Settings Preferences**.
Useful Links	"Infrastructure Settings Preferences Overview" on page 194

The Infrastructure Settings Preferences includes the following elements:

- **General Settings**. Select if you are editing one of the general infrastructure settings in SiteScope.
- **Server Settings.** Select if you are editing settings for the SiteScope server.
- **Monitor Settings.** Select if you are editing settings for various SiteScope monitors.
- **Other Settings.** Select if you are editing settings for the infrastructure properties.

Tips:

- For a description of the elements included in the Infrastructure Settings Preferences, click the **Show Description** button in the upper-right of the Infrastructure Settings Preferences window. Click the button again to hide the descriptions.
- You can find detailed descriptions for some of the infrastructure settings in the Customer Support Knowledge Base. If you are accessing SiteScope standalone, click **Help** > **SiteScope Knowledge Base FAQ**. If you are accessing SiteScope from System Availability Management Administration, click **Help** > **Troubleshooting & Knowledge Base**. Search for Article Number 16186.

Windows Remote Preferences

Description	SiteScope on Windows can monitor systems and services running on remote Windows servers for a large number of statistics without the installation of agent software on each server. This includes monitoring server resources such as CPU, Disk Space, Memory, and Windows-specific performance counter data. Select the servers to display when configuring monitors. SiteScope creates a new remote connection profile for each server address in the list. **To access:** Expand **Preferences** in the monitor tree and click **Windows Remote Preferences**.
Important Information	When configuring particular monitor types, you can display only those servers that have been configured in Remote Preferences by selecting the **Display only configured servers** option.
Useful Links	“Windows Remote Preferences Overview” on page 195

The Windows Remote Preferences includes the following elements:

Main Settings

GUI Element	Description
Host	Enter the IP address or UNC name of the monitored Windows server. An IP host name also works if the SiteScope server is able to translate this common name into an IP address by using a hosts file, DNS, or WINS/DNS integration. To use the same login credentials to configure multiple servers at the same time, enter the server addresses separated by commas. **Example:** If using NetBIOS to connect to other servers in an NT domain, enter a comma-separated string of server addresses such as: \\server1,\\server2,\\server3,\\server4. **Note:** In the list of Windows Remote Preferences servers, use the **Test** button to test connectivity after the profiles have been added. Alternatively, right-click the profile in the monitor tree, and click **Test**.
Login	Enter the login for the remote server. If the server is within the same domain as the SiteScope machine, include the domain name in front of the user login name. For example: <DOMAIN>\<username>. If using a local machine login account for machines within or outside the domain, include the machine name in front of the user login name. For example: <machinename>\<username>.
Password	Enter the password for the remote server or the passphrase for the SSH key file. When using SSH authentication with public/private key based authentication enter the passphrase for the identity file here.
Name	Enter a name by which to identify this remote machine. This name appears in the **Server** list of monitors that can use this connection profile.

GUI Element	Description
Trace	Select to trace messages to and from the subject server, recorded to the SiteScope RunMonitor.log file.
Method	SiteScope uses one of two connection types for monitoring Windows server resources. From the drop-down list select: ➤ **NetBIOS.** The default server-to-server communication protocol for Windows NT and 2000 networks. ➤ **SSH.** Secure Shell, a more secured communication protocol that can be installed on Windows NT/2000 based networks. This connection method normally requires installing SSH libraries on each server to be connected. For more information see the document on Secure Shell in the Advanced SiteScope Topics section.
Remote Machine Encoding	Enter the encoding for the remote server, if the remote server is running an operating system version that uses a different character encoding than the server on which SiteScope is running. This enables SiteScope to display encoded content correctly. **Default:** Cp1252 encoding **Other encodings:** Cp1251, Cp1256, Shift_JIS, EUC_JP

Advanced Settings

GUI Element	Description
SSH Connection Method	Select the client to use for this connection from the list. The currently supported clients are: ➤ Internal Java Libraries. Connect using the Java SSH client integrated with SiteScope. ➤ Plink/External SSH. Connect using an external SSH client. On Windows, SiteScope includes Plink.
SSH Port Number	Enter the port on which the remote SSH server is listening.

GUI Element	Description
Disable Connection Caching	Select to turn off connection caching for this remote. By default, SiteScope caches open connections.
Connection Limit	Enter the number of open connections that SiteScope allows for this remote. If there are many monitors configured to use this connection, set the number of open connections high enough to relieve a potential bottleneck. **Note:** This setting does not effect running tests for a remote server. Tests always create a new connection.
SSH Authentication Method	Select the authentication method to use for SSH connections from the drop-down list. The currently supported methods are: ➤ **Password.** Authenticate using a password. ➤ **Key File.** Authenticate using public/private key authentication. When this option is selected SiteScope uses the private key in the file <**SiteScope root directory**>**/groups/identity** to authenticate. The corresponding public key must be listed in the **authorized_keys** file on the remote host. For more information on SSH requirements, see "SiteScope Monitoring Using Secure Shell (SSH)" on page 1333.
Key File for SSH connections	Select the file that contains the private key for this connection. The default key file is <**SiteScope root directory**>**\groups\identity**. This setting applies only when the authentication method is Key File.
Description	Add a text description for the remote Windows server. This text appears only when editing the remote's properties.

Category Settings

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see "Create and Define a New Category" on page 173.

UNIX Remote Preferences

Description	SiteScope can monitor systems and services running on remote UNIX servers for certain statistics (such as CPU, Disk Space, Memory, and Processes) without the installation of agent software on each server. Select the servers to display when configuring UNIX monitors. SiteScope creates a new remote connection profile for each server address in the list. **To access:** Expand **Preferences** in the monitor tree and click **UNIX Remote Preferences**.
Useful Links	"UNIX Remote Preferences Overview" on page 201

The UNIX Remote Preferences includes the following elements:

Main Settings

GUI Element	Description
Host	Enter the IP address or host name of the monitored server. If using the HTTP method of monitoring, enter the full URL of the CGI script (for example: http://demo.thiscompany.com/cgi-bin/run.sh). To use the same login credentials to configure multiple servers at the same time, enter the server addresses separated by commas. **Example:** If using NetBIOS to connect to other servers, enter a comma-separated string of server addresses such as: serveraddress1,serveraddress2,serveraddress3,serveraddress4 When completing the other required entries on the form, SiteScope creates a new remote connection profile for each server address in the list. **Note:** To test connectivity after the host is added, click **Test** in the table listing the UNIX Servers. This tests only the connection to the server. Click **Detailed Test** to run a test that displays the result of running commands on the remote host. This enables checking the permissions for the defined user.
Login	Enter the login for the remote server.
Password	Enter the password for the remote server or the passphrase for the SSH key file. When using SSH authentication with public/private key based authentication enter the passphrase for the identity file.
Name	Enter a name by which the remote machine should be known in SiteScope. This name appears in the list of the Choose Server page for monitors that can connect to remote servers.
Trace	Select to trace messages to and from the remote server in the **RunMonitor.log** file.

GUI Element	Description
OS	The operating system that is running on a remote server. This is required so that the correct information can be obtained from that server. Select an operating system from the list. For servers running versions of UNIX which are not included in the list, see “UNIX Operating System Adaptors” on page 1323.
Method	The currently supported methods are: ➤ **Telnet.** Log in to the remote server using Telnet. ➤ **SSH.** Log in to the remote server using the SSH protocol. This may require additional software and setup depending on the version of UNIX. For more information on SSH requirements, see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1333. ➤ **Rlogin.** Log in to the remote server using the Rlogin protocol. ➤ **HTTP.** Connect to an HTTP server on the remote server and run the command via a CGI. For this method the Login and Password are optional and are used for authorizing SiteScope to log on to the remote machine if required. For more information, see “Connection Methods for Remote UNIX” on page 202
Prompt	This is the prompt output when the remote system is ready to handle a command. **Default: #**
Login Prompt	This is the prompt output when the system is waiting for the login to be entered. **Default:** login:
Password Prompt	This is the prompt output when the system is waiting for the password to be entered. **Default:** password:

GUI Element	Description
Secondary Prompt	Enter the secondary prompts if the telnet connection to the remote server causes the remote server to prompt for more information about the connection. Separate multiple prompt string by commas (,). **Example:** For Telnet connections to some remote servers, the remote server may ask what terminal type should be emulated for the connection. In this case, enter Terminal type? as the secondary prompt. The response to the secondary prompt is entered in the Secondary Response box below.
Secondary Response	Enter the responses to any secondary prompts required to establish connections with this remote server. Separate multiple responses with commas (,).

GUI Element	Description
Initialize Shell Environment	Enter any shell commands to be executed at the beginning of the session. Separate multiple commands with a semicolon (;). This option specifies shell commands to be executed on the remote machine directly after a Telnet or SSH session has been initiated. These commands can be used to customize the shell for each SiteScope remote. Some examples include: ➤ The remote shell may not have the correct path set for SiteScope scripts to run. The following command adds the directory **/usr/local/bin** into the PATH of the current shell on the remote machine: export PATH=$PATH:/usr/local/sbin ➤ The remote shell may not be initializing the pseudo terminal correctly. Enter the following command to increase the terminal width to 1024 characters: stty cols 1024;${SHELL} **Note:** Commands after a shell invocation are not executed. ➤ There have been cases where the remote Telnet Server does not echo back the command line properly. This may cause strange behavior for monitors that rely on this behavior. Enter the following command to force the remote terminal to echo: stty echo ➤ Certain UNIX shells have been known to behave erratically with SiteScope. This includes bash, ksh, and csh. Enter the following command to change the shell to sh for the SiteScope connection: /bin/sh
Remote Machine Encoding	Enter the encoding for the remote server if the remote server is running an operating system version that uses a different character encoding than the server on which SiteScope is running. This enables SiteScope to display encoded content correctly. **Default:** Cp1252 encoding **Other encodings:** Cp1251, Cp1256, Shift_JIS, EUC_JP

Advanced Settings

GUI Element	Description
SSH Connection Method	Select the client to use for this connection from the list. The currently supported clients are: ➤ **Internal Java Libraries.** Connect using the Java SSH client integrated with SiteScope. ➤ **Plink/External SSH.** Connect using an external SSH client. On Windows, SiteScope includes Plink. On Solaris or Linux SiteScope uses an installed client such as OpenSSH.
SSH Port Number	Enter the port on which the remote SSH server is listening.
Disable Connection Caching	Select to turn off connection caching for this remote. **Default:** SiteScope caches open connections.
Connection Limit	Enter the number of open connections that SiteScope allows for this remote. If there are many monitors configured to use this connection, set the number of open connections high enough to relieve a potential bottleneck. **Note:** This setting does not effect running tests for a remote server. Tests always create a new connection.
SSH Authentication Method	Select the authentication method to use for SSH connections from the list. The currently supported methods are: ➤ **Password.** Authenticate using a password. ➤ **Key File.** Authenticate using public/private key authentication. When this option is selected, SiteScope uses the private key in the file **SiteScope/groups/identity** to authenticate. The corresponding public key must be listed in the **authorized_keys** file on the remote host. For more information on SSH requirements, see “SiteScope Monitoring Using Secure Shell (SSH)” on page 1333.

GUI Element	Description
Key File for SSH connections	Select the file that contains the private key for this connection. The default key file is **SiteScope\groups\identity**. This setting applies only when the authentication method is Key File.
SSH Version 2 Only	Check this option to force SiteScope to use SSH protocol version 2 only. This option applies only when using the integrated Java Client. For information on configuring an external SSH client to use SSH2 protocol, see "Using an External SSH Client" on page 1358.
Custom Commandline	Enter a custom command line for a remote server using the External Client. Use this option when passing specific commands to the external client, to be executed. Valid substitution variable are: ➤ **$root$.** This translates the SiteScope directory. ➤ **$user$.** This translates the username entered into the remote server. ➤ **$password$.** This translates the password entered into the remote server. ➤ **$host$.** This translates the host name entered into the remote server.
Description	Add a text description for the remote UNIX server. This text appears only when editing the remote's properties.

Category Settings

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the Categories tab. For details, see "Create and Define a New Category" on page 173.

Log Preferences

Description	Effective system availability monitoring requires that monitoring data be recorded and stored for an appropriate interval of time. SiteScope Log Preferences controls the accumulation and storage of monitor data. **To access:** Expand **Preferences** in the monitor tree and click **Log Preferences**.
Useful Links	"Log Preferences Overview" on page 204

The Log Preferences includes the following elements:

Main Settings

GUI Element	Description
Daily Logs To Keep	Enter the number of days of monitoring data to keep. Once a day, SiteScope deletes any logs older than the specified number of days. **Default:** 40 days, enough data to create monthly reports. **Note:** Keeping monitor data logs for long periods can cause a data storage problem for the SiteScope server depending on the total number of monitors configured and how often the monitors run per day. You should monitor the size of the log files in the **SiteScope\logs** directory to estimate the data accumulation rate and adjust the **Daily Logs To Keep** setting or server resources as necessary.
Maximum Size of Logs	Enter the maximum size allowed for all monitoring logs. Once a day, SiteScope checks the total size of all monitoring logs and removes any old logs that are over the maximum size. **Default:** No value. **Note:** By default, this setting is blank and not used as it can result in the loss of monitor report data.

GUI Element	Description
Database Connection URL	To enable Database logging, enter a URL to a Database Connection. The easiest way to create a database connection is to use ODBC to create a named connection to a database. **Example:** First use the ODBC control panel to create a connection called SiteScopeLog. Then, enter jdbc:odbc:SiteScopeLog in this box as the connection URL. **Note for using Windows Authentication:** If you want to access the database using Windows authentication, enter jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>; AuthenticationMethod=type2 as the connection URL, and com.mercury.jdbc.sqlserver.SQLServerDriver as your database driver. Leave the **Database User Name** and **Database Password** boxes empty, since the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.
Database Driver	Specify the database driver SiteScope should use to connect to the database. The driver should be a JDBC driver. To have SiteScope use another driver the driver must also be installed in the <**SiteScope install path**>**/WEB-INF/lib** directory and the path and filename must be entered in this box. **Default database driver:** sun.jdbc.odbc.JdbcOdbcDriver.
Database Username	Enter the username used to log in to the database. If using Microsoft SQL server, leave this blank and choose NT Authentication when setting up the ODBC connection. With NT Authentication, SiteScope connects using the login account of the SiteScope service.

GUI Element	Description
Database Password	Enter a password used to login to the database. If using Microsoft SQL server, leave this blank and choose NT Authentication when creating the ODBC connection. With NT Authentication, SiteScope connects using the login account of the SiteScope service.
Backup Database Connection URL	(Optional) Enter a URL to a backup database. Use this option to provide failover of SiteScope database logging if the primary database becomes unavailable. **Note:** The same database table definition, database driver, user name, and password are applied to both database connections. After saving changes to the Database preferences, stop and restart the SiteScope service for the changes take effect.

E-mail Preferences

Description	E-mail is the default media for sending event alerts when a problem has been detected by SiteScope (in addition to the visual icons and status messages displayed in the SiteScope interface). Use the E-mail Preferences to indicate the SMTP mail server, recipient addresses, and other settings that SiteScope should use when sending e-mail alerts and other SiteScope messages. **To access:** Expand **Preferences** in the monitor tree and click **Mail Preferences**.
Useful Links	"E-mail Preferences Overview" on page 207 "E-mail Recipient Profile Settings" on page 255

The E-mail Preferences includes the following elements:

Main Settings

GUI Element	Description
E-Mail Server Domain Name	Enter the domain name of the SMTP mail server that SiteScope should use when sending e-mail messages. **Example:** mail.thiscompany.com If you are unsure of your mail server's domain name, check with your Systems Administrator.
Administrator E-mail Address	Enter the e-mail address to which SiteScope should send status messages. **Example:** sysadmin@thiscompany.com
Daily Status	Select this option to have SiteScope send a brief daily status message to the administrator's e-mail address. This e-mail is scheduled to be generated at 7:07 AM every day. The subject of e-mail sent includes: "SiteScope daily status". The e-mail content includes the number of active monitors and groups, along with a URL link to the applicable SiteScope main page plus the version number of SiteScope installation.
SiteScope Starts/Restarts	Select this option to have SiteScope send a brief message each time that SiteScope restarts. Normally, SiteScope automatically restarts itself once a day. Other restarts may be an indication of a monitor run problem. For more information, see “Monitoring SiteScope Server Health” on page 293.
From E-mail Address	Enter the e-mail address used as the From Address for mail generated by SiteScope. Specifying an e-mail address may make it easier to browse and sort e-mail sent by SiteScope. If nothing is entered, the **From E-mail Address** stays the same as the address where the mail is sent from. **Example:** sitescope@mycompany.com **Note:** If the mail server being used required NTLM authentication (see below), the e-mail address entered here must be a valid e-mail address.

GUI Element	Description
Backup Mail Server Domain Name	Enter the domain name of the SMTP mail server that SiteScope should use whenever the primary mail server cannot be reached. If unsure of backup mail server's domain name, check with the Systems Administrator. **Example:** gateway.mycompany.com.
Login	Enter the username required by the SMTP server in this field. This user name is used for both the primary and backup mail servers.
Password	If the SMTP server you want SiteScope to use requires authentication, enter the password for username entered in the **Login** field. This password is used for both the primary and backup mail servers.
NTLM Authentication	Select an NTML authentication option from the drop-down list: ➤ **None**. Select if the mail server does not require NTLM authentication. ➤ **NTLMv1**. Select if the mail server requires authentication using NTLM version 1. ➤ **NTLMv2**. Select if the mail server requires authentication using NTLM version
Timeout	Enter an optional length of time (in seconds) to wait for a response from the SMTP server. If a response from the primary mail server is not received within the timeout period, SiteScope switches to use the backup mail server. **Default value:** 60 seconds. This is also the minimum value.

E-mail Recipient Profile Settings

Description	The E-mail Recipients page lists E-mail Recipient profiles that you use with SiteScope E-mail Alerts. Create and use the E-mail Recipient profiles for sending SiteScope e-mail alerts to individuals or groups other than the SiteScope Administrator e-mail entered on the E-mail Properties. **To access:** Expand **Preferences** in the monitor tree and click **Mail Preferences**. Click **New E-Mail Recipient**.
Useful Links	"E-mail Preferences Overview" on page 207 "E-mail Preferences" on page 252

The E-mail Recipient Profile includes the following elements:

Main Settings

GUI Element	Description
Name	Enter a text description for the E-mail Recipient Profile definition. The name is used to identify the E-mail Recipient Profile definition in the product display.
E-mail To	The e-mail addresses to which you want to send the alert. **Example:** test@mycompany.com You can enter multiple e-mail addresses by separating the e-mail addresses with commas. **Example:** test@mycompany.com, sysadmin@thiscompany.com
Disabled	Stops e-mail alerts from being sent to these e-mail addresses. Use this option to temporarily disable a particular e-mail without editing every alert that contains this e-mail setting.

Advanced Settings

GUI Element	Description
Template	Select a template from the drop-down list to define the e-mail alert settings. Once a setting is defined, a single alert is sent to people and pagers. Use the **ShortMail** template for pagers.
Schedule	Use this option to specify when e-mail settings should be enabled. You may select a more restricted schedule from the names schedules in the drop-down menu. **Default:** every day, all day
Description	Enter a description for the setting profile, which appears only when editing or viewing its properties.

Category Settings

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the **Categories** tab. For details, see "Create and Define a New Category" on page 173.

Pager Preferences

Description	Pager Preferences configures settings and additional pager profiles that SiteScope uses for sending Pager alerts. ➤ Sends an automated notification to system administrators who may not have immediate access to e-mail. ➤ Sends alert escalation or notifies support personnel who may be away from the office. **To access:** Expand **Preferences** in the monitor tree and click **Pager Preferences**.
Useful Links	"Pager Preferences Overview" on page 208 "Pager Recipient Profiles" on page 260

The Pager Preferences includes the following elements:

Main Settings

GUI Element	Description
Modem Port	Select the communications port that the modem is connected to on the SiteScope server. For SiteScope on Solaris or Linux, enter the path and device name for the modem. On Windows NT/2000 platforms, SiteScope uses COM port numbers for both RS-232C type serial ports as well as for USB modem ports. If you are using a USB type modem, select the COM port associated with the USB port to have SiteScope use the USB modem. To find the COM port number for the USB modem, use the **Settings** > **Network and Dial-up Connections** menu. Right-click the desired modem, and then click **Properties**. The properties should show the COM port number that is associated to the modem.

GUI Element	Description
Connection Speed	Select the modem speed used for connections to the paging service from the drop-down list. **Default:** 1200 baud
Pager Connection Options	Select an option for sending a message to your paging service: ➤ **Modem-to-Modem Connection (preferred).** Select if you have an alphanumeric pager and use an alphanumeric paging service. ➤ **Dial and Enter Message.** Select to dial a direct phone number to send a page. ➤ **Dial, Enter Command, and Enter Message.** Select if you have a direct number, but need to enter a command before sending a page. ➤ **Custom Modem Connection.** Select if your paging company does not use any of the previous connection choices. For the information required for the selected option, see the table below.

Pager Connection Options

Enter the information required for the selected Pager Connection option:

GUI Element	Description
Modem number	Type the phone number to use for sending alphanumeric pages to the paging service modem.
Modem pin number	Type the last seven digits of the PIN number for your alphanumeric pager. For a list of numbers, see "Modem Numbers" on page 208.

GUI Element	Description
Phone number	Type the phone number exactly as you would dial it from your telephone, including other numbers you might need, such as a number to get an outside line. You can use dashes to make the number easier to read. Use commas to separate the portions of the phone number. Each comma causes the modem script to pause for a few seconds before dialing the rest of the number. **Example:** If you are dialing your pager from your office, and you have to dial 9 to get an outside line, type: 9, 555-6789.
Send page command	Type the page command exactly as you would dial it from your touch tone telephone.
Custom Modem command.	Type the entire modem command including the phone number to dial, any additional digits, and $message. SiteScope replaces $message with the message you specified for each alert. **Example:** If the number for the pager company is 123-4567, your pager PIN is 333-3333, and your pager company requires that you follow each command with the # key, the command might look like this: ATDT 123-4567,,333-3333#,,$message# **Note:** For SiteScope running on UNIX, enter the device path for your modem in the **Modem Path** box. To see a list of devices using Solaris, use the ls /dev/term/* command.

Pager Recipient Profiles

Description	The Pager Recipients Contents view lists Pager Recipient profiles that can be used with SiteScope Pager Alerts. This view lists the name of all the currently defined Pager settings or profiles. Create and use different Pager Recipient profiles for sending SiteScope Pager alerts to individuals or groups other than the one defined in the Pager Recipient Properties. **To access:** Expand **Preferences** in the monitor tree and click **Pager Preferences**. Click **New Pager Recipient**.
Useful Links	"Pager Preferences Overview" on page 208 "Pager Preferences" on page 257

The Pager Recipient Profiles includes the following elements:

Main Settings

GUI Element	Description
Name	Enter the text name string assigned to the setting profile when you create a new pager recipient.
Connection Speed	Select the modem speed used for connections to the paging service from the drop-down menu list. **Default:** 1200 baud

GUI Element	Description
Pager Connection Options	There are four options for sending a message to your paging service: ➤ Modem-to-Modem Connection (preferred) ➤ Dial and Enter Message ➤ Dial, Enter Command, and Enter Message ➤ Custom Modem Connection The **preferred option** is to connect directly to a **modem at your pager service**. When a modem-to-modem connection is used, SiteScope is able to verify that the message was sent successfully and can receive messages describing any communication problem. The other connection options generally send messages to automated voice response systems using touch tone dialing. The touch tone dialing method is limited to numeric messages and SiteScope cannot confirm that your paging service correctly received the message. For more information on the different options, see “Pager Preferences Overview” on page 208.
Disabled	Select to temporarily disable a particular pager without editing every alert that contains this persons pager.

Advanced Settings

GUI Element	Description
Schedule	Specifies when pager settings should be enabled. A more restricted schedule can be selected from the drop-down list. **Default:** every day, all day
Description	Enter a description for the setting profile, which appears only when editing or viewing its properties.

Category Settings

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the **Categories** tab. For details, see "Create and Define a New Category" on page 173.

SNMP Trap Preferences

Description	With the diversity of business systems and applications available, the interoperability of management applications can be important to overall system effectiveness and manageability. SiteScope can integrate with SNMP-based network management systems by using the SiteScope SNMP Trap Alert type. Use the SNMP Trap Preferences to define settings that are used by SiteScope SNMP Trap alerts when sending data to management consoles. **To access:** Expand **Preferences** in the monitor tree and click **SNMP Preferences**.
Useful Links	"SNMP Trap Preferences Overview" on page 209

The SNMP Trap Preferences includes the following elements:

Main Settings

GUI Element	Description
Name	Enter the text name string assigned to the setting profile when creating a new SNMP recipient.
Send to Host	Enter the domain name or IP address of the machine that receives all SNMP trap messages. This machine must be running an SNMP console to receive the trap message. **Examples:** snmp.mydomain.com or 206.168.191.20.

GUI Element	Description
SNMP Port	The SNMP port to which the trap is sent.
SNMP Community	The default SNMP community name used for sending traps. The community string must match the community string used by the SNMP management console. **Default:** public
SNMP Trap ID	The type of trap to send. There are several predefined ID types for common conditions. ➤ Select a generic SNMP type from the **Generic SNMP Trap ID** drop-down list. ➤ To use an enterprise specific SNMP ID type, enter the number of the specific trap type in the **Enterprise-Specific SNMP Trap ID** box.
SNMP Trap Version	Select the default SNMP protocol version number to use. SNMP v1 and v2c are currently supported.
SNMP Object ID	This identifies to the console the object that sent the message. ➤ Select one of the predefined objects from the **Preconfigured SNMP Object IDs** drop-down list. ➤ To use another object ID, enter the other object ID in the **Other SNMP Object ID** box.

Advanced Settings

GUI Element	Description
Description	Enter a description for the setting profile, which appears only when editing or viewing its properties.

Category Settings

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the **Categories** tab. For details, see “Create and Define a New Category” on page 173.

Dynamic Update Preferences

Description	When infrastructure is added, operational monitoring needs to be configured. Any breakdown in the communication of these changes can lead to gaps in monitoring coverage and increased operational vulnerability. The Dynamic Update feature integrates SiteScope with other management tools and dynamically deploys server monitoring. **To access:** Expand **Preferences** in the monitor tree and click **Dynamic Update Preferences**.
Useful Links	“Dynamic Update Preferences Overview” on page 210

The Dynamic Update Preferences includes the following elements:

Main Settings

GUI Element	Description
Template Set	Select the **Monitor Set Template** to be used when creating new monitors for any new hosts detected by the SiteScope Dynamic Update. The template used for the Dynamic Update feature should be constructed so that the server IP address is the only input required to create the monitors in the set. See the **Monitor Set Templates** in the SiteScope Reference Guide for more information.

GUI Element	Description
Monitor Set Subgroup Name	Define the group name to be applied to each new group of monitors, created with the Monitor Set Template above. Normally, a new monitor group is created for each new IP address detected by the Dynamic Update. The default group name defined by $NODE-IP$ is the IP address of the node or server. Add a text string to the group name box to be included in the group name. **Example:** $NODE-IP$ Server Group **Note:** It is recommended to include the $NODE-IP$ variable as part of the group name field to ensure that a unique subgroup name is created and to avoid possible problems of duplicate group names. (Optional) All the monitors created by the Dynamic Update can be added as individual monitors to the group specified in the **Group Name** box below, by deleting the contents of this box and leaving it blank.
Group Name	Enter a text string as the group name to be created as a container group for all monitor subgroups created using this Dynamic Update Set.
Parent Group	Use the expandable menu tree to select an existing SiteScope group to which the above container group is added as a subgroup.
Update Frequency	Enter the frequency, in seconds, that the SiteScope Dynamic Update should check the SNMP MIB or database for new IP addresses. It is possible to calculate a frequency value equivalent to many hours, or even days, depending on the rate that servers are being added to the network. To discontinue a Dynamic Update, delete the set definition from the Dynamic Update Set table.

GUI Element	Description
Exclude IP	Enter any IP addresses to be excluded from the Dynamic Update Set. To exclude multiple IP addresses, enter them into the text box and separate them by commas. To exclude a range of IP addresses, use the * (asterisk) wildcard character. **Example:** You may want to exclude the default gateway IP if it represents a load balancing server or device. Enter 12.3.4.* to exclude all IP addresses in the range 12.3.4.0 to 12.3.4.999 range.
Name	Optional name for this Dynamic Update Set. The default name is the template set name with either the server address or database server name.

SNMP MIB Search

GUI Element	Description
Server Address	The server address or console where the SNMP MIB is found. Enter the address as a UNC name. **Example:** \\servername or the IP address of the server
SNMP Object ID	Select the root OID for the SNMP object that returns the node IP addresses to be monitored by the Dynamic Update. Use the selection box for the default OID for F5 Big-IP servers or select the **other** option and enter the Object ID information in **Other SNMP OID** below.
Other SNMP OID	Enter the root OID for the object that returns the node IP addresses to be monitored if you selected **other** in **SNMP Object ID** above.
Community	Enter the community variable for the SNMP MIB. **Default:** public

Database Search

GUI Element	Description
Database Connection URL	Enter a URL to a Database Connection. The easiest way to create a database connection is to use ODBC to create a named connection to a database. **Example:** First use the ODBC control panel to create a connection called test. Then, enter jdbc:odbc:test in this box as the connection URL. Save the changes and then complete the Database Search section.
Database Driver	Enter the Java class name of the JDBC database driver used for database connections. The sun.jdbc.odbc.JdbcOdbcDriver uses ODBC to make Database connections. The com.inet.tds.TdsDriver can be used to connect to Microsoft SQL Server databases. If a custom driver is used, the driver must also be installed in the **<SiteScope install path>/SiteScope/java** directory.
SQL Query	Enter the SQL query to run against a table in the database specified above that returns the list of IP addresses to be monitored. This database table should be a table that is used to record the server addresses that are currently in the network or are added to the network. The table records must include a field containing the server UNC name or IP address without any additional text or description in the same field.
Database Username	Enter the user name used to log in to the database.
Database Password	Enter the password used to log in to the database as the user entered above.
Query Timeout	Enter a timeout value, in seconds, that SiteScope should wait for a database query to return results.

Category Settings

GUI Element	Description
Assigned categories	Assign a category to this element for use when filtering the monitor tree. To define new categories, select the **Category** tab at the top of the SiteScope page. To filter the monitor tree, select the Views tab.

Advanced Settings

GUI Element	Description
Description	Enter a description for this Dynamic Update Set, which appears only when editing or viewing its properties.

Absolute Schedule Preferences

Description	Absolute Schedule Preferences allows customizing the operation of SiteScope monitors and alerts to run only at specific times. **To access:** Expand **Preferences** in the monitor tree and click **Absolute Schedule Preferences**.
Useful Links	"Absolute Schedule Preferences Overview" on page 211

The Absolute Schedule includes the following elements:

Main Settings

GUI Element	Description
Name	Enter a name for the Absolute Schedule. The name is used to identify the Absolute Schedule in the product display.
Days of the Week	Enter the time or times that the monitor needs to run in the boxes next to the day of the week. Time values for absolute schedules must be limited to the 24-hour period of a standard day for each day. To enter multiple times for a single day, separate the times by a comma (,). **Example:** 01,02:30,23:30 runs the monitor at 1:00 AM, 2:30 AM, and 11:30 PM

Advanced Settings

GUI Element	Description
Description	Enter a description for the setting profile, which appears only when editing or viewing its properties.

Category Settings

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the **Categories** tab. For details, see “Create and Define a New Category” on page 173.

Range Schedule Preferences

Description	SiteScope Range Schedule Preferences allows customizing the operation of SiteScope monitors and alerts to fit special schedule requirements of the operation and the organization. **To access:** Expand **Preferences** in the monitor tree and click **Range Schedule Preferences**.
Useful Links	"Range Schedule Preferences Overview" on page 212

The Range Schedule Preferences includes the following elements:

Main Settings

GUI Element	Description
Name	Enter a name for the Range Schedule.
Days of the Week	In the boxes next to the day of the week, select **Enabled** or **Disabled** and enter the time or times the monitor needs to run. Time values for range schedules must be limited to the 24-hour period of a standard day for each day. **Example:** To disable monitors from 6:00 PM on Thursday evening until 8:00 AM the following morning, enter a **From** value of 18 to 24 for Thursday and then enter from 0 to 8 for Friday. If you enter a **From** value of 18 and a **To** value of 8 on the Thursday schedule, the schedule becomes invalid. To enter multiple times for a single day, separate the times by a comma (,). For example, to disable from 2-3AM and 7-8AM, enter 2:00,3:00 to 7:00,8:00. **Default:** Enabled (no time values specified). See the table below for more information.

Days of the Week

Enable Setting (Enable / Disable)	Time Range (From /To)	Schedule Effect
Enable	**From** and **To** time values specified	Monitors are enabled to run only during the **From** and **To** time range.
Enable	(no time values specified)	Monitors are enabled to run during all hours of the applicable day. This is the default setting for 24-hour operation.
Disable	**From** and **To** time values specified	Monitors are enabled to run during all hours of the applicable day, except during the **From** and **To** time range.
Disable	(no time values specified)	Monitors are disabled during all hours of the applicable day.

Advanced Settings

GUI Element	Description
Description	Enter a description for the setting profile, which appears only when editing or viewing its properties.

Category Settings

GUI Element	Description
Assigned categories	Assign a category for use when filtering the monitor tree. To define new categories, click the **Categories** tab. For details, see "Create and Define a New Category" on page 173.

User Preferences

Description	The data provided by SiteScope can be made available to multiple users without granting full administrative privileges to all users. This page allows you to create multiple user accounts that provide different view and edit permissions for different audiences. **To access:** Expand **Preferences** in the monitor tree and click **Users Preferences**.
Useful Links	"User Preferences Overview" on page 213

The User Preferences includes the following elements:

Main Settings

GUI Element	Description
Login Name	Enter the SiteScope login name to access SiteScope using this profile. Alternatively, users can log into SiteScope using LDAP authentication by entering a value in the LDAP fields below. **Allowed characters**: Latin alphanumeric. **Note**: Entering characters other than the allowed characters does not cause an error when creating the user profile. However, the user cannot log in to SiteScope using that login name.

GUI Element	Description
Password	Enter the SiteScope login password for this user. If using LDAP for user authentication, there is no need to enter a password here. Users enter their LDAP password in the SiteScope login dialog box when they log in to their user account. For information on password requirements, see "Change a User's Password" on page 222. All SiteScope passwords are encrypted using 3DES (also known as TDES or Triple Data Encryption Algorithm). For more information, refer to "Hardening the SiteScope Platform" in the *HP SiteScope Deployment Guide* PDF.
Confirm Password	Re-enter the password entered in the **Password** box. This is used when creating a new user profile or changing the password of an existing user profile.
LDAP Service Provider	To access the SiteScope service using a centralized LDAP authentication rather than the SiteScope specific password, enter the URL of the applicable LDAP server. This way, password authentication for access to SiteScope can be performed by LDAP. **Example:** ldap://ldap.mydomain.com:389. **Note:** ➤ Users still need to have a SiteScope login name defined. ➤ Users can use LDAP to access SiteScope, but they must have a user login and security principal assigned to them on the LDAP server.
LDAP Security Principal	When using LDAP authentication to access the SiteScope service, enter the Security Principal for this user. **Example:** uid=testuser,ou=TEST,o=this-company.com **Note:** Users may be defined with special characters on the LDAP server. However, SiteScope does not support users that contain the following characters in their user name: equal ("="), semi-colon (";"), inverted commas (""").

GUI Element	Description
Title	(Optional) Enter a title for this User profile. The title is displayed in the list of users. If you do not enter a title, the **Login Name** value is used as the Title.
Allowed Groups	Use the expandable menu tree to select the monitor groups that can be accessed by this user profile. Select the groups the user is allowed to access. Select the box next to individual groups or subgroups to allow access to that group. To restrict user access to fewer groups, clear the check box for the SiteScope node and then select the individual groups below the SiteScope node to which you want to allow access. **Default:** The SiteScope node is checked to allow access to all groups.
Login Disabled	Select to disable access to SiteScope with this username and password. Clear the check box to enable access using the user profile.

Enable Editing/Deleting User Preferences

GUI Element	Description
Enable edit users	Enables the user to edit or delete user preferences for all other users, except the SiteScope administrator user.

Group Actions

GUI Element	Description
Edit Groups	Enables the user to add new groups, rename, copy, or delete existing monitor groups.
Refresh Groups	Enables the user to refresh or force all the monitors within a group to run regardless of their schedule.
Disable Groups	Enables the user to disable groups.

Monitor Actions

GUI Element	Description
Edit Monitors	Enables the user to add new monitors, edit existing monitor configurations, or delete monitors.
Refresh Monitors	Enables the user to refresh or force individual monitors to run regardless of their schedule.
Acknowledge Monitors	Enables the user to use the Acknowledge feature to comment on monitor status on the group detail page.
Disable Monitors	Enables the user to disable monitors within a group.
Use Monitor Tools	Enables the user to use the Diagnostic Tools form for certain monitor types. When a diagnostic tool is available for a monitor type, a hyperlink is presented in the More column for that monitor in the group detail page. Diagnostic tools may expose sensitive system information.

Alert Actions

GUI Element	Description
View Alerts List	Enables the user to view the list of currently configured alert definitions on the Alert List page.
Edit Alerts	Enables the user to add a new alert, edit, or delete existing alerts.
Test Alerts	Enables the user to test an existing alert definition.
Disable Alerts Indefinitely	Enables the user to disable or enable one or more alerts indefinitely.
Disable Alerts Temporarily	Enables the user to disable or enable one or more alerts temporarily.
Create Adhoc Alert Reports	Enables the user to create adhoc or quick alert reports using the **Alert Report** link below the Alert Definitions table.

Report Actions

GUI Element	Description
Generate Reports	Enables the user to generate a scheduled report manually.
Edit Reports	Enables the user to add new report definitions, and edit or delete existing report definitions.
Create Adhoc Reports	Enables the user to use the Quick Report action on the Management Reports page to create ad hoc reports.
Disable Reports	Enables the user to disable or enable the generation of existing reports.
View Monitor History Report	Enables the user to view the recent history report for a monitor.

Preference Settings

GUI Element	Description
Edit Preferences	Enables the user to use any of the forms available on the Preferences submenu to add or edit SiteScope settings for e-mail alerts and other SiteScope messages, logging, integration, connectivity to remote servers, and so forth.
Test Preferences	Enables the user to test any preference setting that is testable. This is usually a setting for communicating with an external service such as e-mail, modem, SNMP, or other external application.

View Options

GUI Element	Description
View View	Enables the user to view the Views page to see a list of defined views.
Edit View	Enables the user to add, edit, or delete views and view settings.

Categories Options

GUI Element	Description
View Category	Enables the user to view the Categories page to see a list of defined categories.
Edit Category	Enables the user to add, edit, or delete categories and category settings.

Templates Options

GUI Element	Description
View Templates	Enables the user to view templates that exist in the monitor tree.
Edit Templates	Enables the user to add, edit, deploy, and delete templates.

Other Options

GUI Element	Description
Use Tools	Enables the user to view and use the tools in the Tools container.
Use Browse and Summary	Enables the user to use the Browse Monitor form and the Monitor Summary Report.
View Progress	Enables the user to view the progress page showing monitors that are running and SiteScope monitoring load.
View Logs	Enables the user to view the raw data reported by SiteScope monitors, sent by alerts, and other SiteScope logs.

Dashboard Options

GUI Element	Description
Edit Favorites	Enables the user to add or delete items in the favorite views list in the Dashboard view.

15

Global Search and Replace User Interface

This chapter includes the pages and dialog boxes that are part of Global Search and Replace in the SiteScope environment.

This chapter describes:	On page:
Global Search and Replace Wizard	279

Global Search and Replace Wizard

Description	Global Search and Replace enables you to make changes to monitor, alert, group, preferences, alert action, and report properties. These changes can be made across an entire SiteScope infrastructure when working in SiteScope standalone or across several SiteScopes when working in System Availability Management Administration. **To access:** In SiteScope standalone, right-click the group, preferences, alert, or monitor in the monitor tree to which you want to perform the global replace, and select **Global Replace** from the menu. In System Availability Management Administration, select **Admin** > **System Availability Management** and click the **Global Search and Replace** button.

Wizard Map	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.

The following elements, listed in alphabetical order, are found throughout the Global Search and Replace wizard:

GUI Element	Description
<wizard steps>	All steps of the wizard are visible in the left-hand pane. An arrow points to your current step.
Back	You can navigate to any earlier step in the wizard. If you make a change in any prior entry, all entries made in the succeeding pages are removed.
Cancel	You can exit the wizard without making any changes.
Finish	Whatever replacement you chose in earlier steps in the wizard are done. It is not possible to undo the replacement once you click **Finish**.
Help	Opens a new window with further explanations.
Next	You can navigate to the next step in the wizard.

Select SiteScope Page

Description	Use the Select SiteScope Page to select the SiteScope upon which to make replacements.
Important Information	Only SiteScopes running version 9.0 and higher and whose connection status allows configuration changes from System Availability Management are listed. You must select at least one SiteScope.
Wizard Map	The Global Search and Replace wizard includes: **Select SiteScope Page** (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.

Select Type Page

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

The page includes the following elements:

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

Select Subtype Page

Description	Use the Select Subtype page to select the properties of the object type upon which you want to make replacements.
Important Information	This page opens only if you selected **Alert Action, Monitor**, or **Preferences** as the object type in the Select Type Page of the wizard. If you selected the object type **Group** or **Report**, this page does not open.
Wizard Map	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > **Select Subtype Page** > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > Summary Page.

The page includes the following elements:

GUI Element	Description
☑ □ ⇄	You can use these options to select all listed SiteScopes, clear the selection, or invert the current selection so that objects that were selected are cleared and objects that were cleared are selected.

Replace Mode Page

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

The page includes the following elements:

GUI Element	Description
	Optionally, click to open the Advanced Filter dialog box if you want to further refine your selections. You can select objects based on their specific settings and not only based on object type. The Advanced Filter page opens with setting areas pertinent to the object you selected. For details about these settings, refer to the selected object's settings page. **Examples**: ➤ Select all monitors with frequency set to 5 minutes and replace any setting for those monitors. ➤ Select all alerts that have a defined category of critical and replace any setting for those alerts. ➤ Select all groups with a dependency set to a specific monitor or group and replace any setting for those groups. **Note**: Using the Advanced Filter option merely refines your selection for the replace and does not determine what to replace.
Find and Replace	Select to search the target objects for properties that match a string or regular expression and replace only the matching pattern with the replacement value. This method of replacement includes a search for specific settings and property values and replaces only those objects with the entered setting or value. You can select only a partial value and replace only that string. **Example**: Search for all monitors whose name value includes a server name that is no longer in use. Replace the string representing the old server with a new string representing the updated server. **Note**: Use this setting to determine the selection and the value to replace. It differs from the Advanced Filter option which is a way to limit the selected objects but not the value to replace.

GUI Element	Description
Replace	Globally replaces all matching objects with the new string or value.

Choose Changes Page

Description	Use the Choose Changes page to select what to replace for the global replace. The wizard displays only the settings and properties that may be changed for the object type selected in the previous pages. The filter criteria is built from your selections in the Type, Subtype, and Advanced Filter pages.
Important Information	The subtype's properties may be displayed differently than how they are displayed when editing a monitor, alert, preference, and so forth in SiteScope. **Examples**: **Mail Preferences** is a text box in Global Search and Replace utility rather than a drop-down list, and the **Depends On** property is not displayed in the Global Search and Replace utility. **Note for users of SiteScope within System Availability Management Administration**: ➤ If you select SiteScope as the object type, properties of all selected subtypes of the selected SiteScopes are included in this page. ➤ If the SiteScopes selected for the replace operation are not all the same version, the subtypes of the SiteScopes may have different properties.
Wizard Map	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > **Choose Changes Page** > Affected Objects Page > Review Summary Page > Summary Page.

The page includes the following elements:

GUI Element	Description
<Settings area>	This area includes the settings for the object you selected. For details about these settings, refer to the selected object's settings page. ➤ If you selected **Find and Replace** in the Replace Mode page, you must select only the setting in the settings area. Enter the value to replace in the **Find**/**Replace with** fields. ➤ If you selected **Replace** in the Replace Mode page, you must select the setting and the value to replace in the settings area.
Find **Replace With**	If you chose the **Find and Replace** option in the Replace Mode page, the text boxes **Find** and **Replace With** are added to the top of this page. ➤ In the **Find** field, enter the search string, value, or regular expression pattern for the setting or property you want to replace. ➤ In the **Replace With** field, enter the string or value to which you want all matching patterns to be changed. **Note:** If you select **Frequency** in Main Settings drop-down list, the values you enter in the **Find** and **Replace With** text boxes must be in seconds. For example, you want to find monitors with a frequency of 10 minutes and change the frequency to 20 minutes. In the **Find** text box, enter 600 and in the **Replace With** text box enter 1200. If no objects are found that meet the filter criteria, an error message is given. Reselect your filter criteria.

Affected Objects Page

Description	Use the Affected Objects page to view the objects that you selected to change. The page displays the selected objects in tree format. You can clear or select objects in the Affected Objects tree for the replacement operation. ➤ If you selected **Find and Replace** in the Replace Mode page, replacements are made only if the filter criteria are matched. ➤ If you selected **Replace**, replacements are made in all selected objects.
Important Information	The objects displayed depend on whether the user has change permissions on those objects. ➤ When in System Availability Management Administration, the permissions are set in Business Availability Center's Permissions Management (**Admin** > **Platform** > **Users and Permissions**). ➤ When in SiteScope standalone, the permissions are set in **Preferences** > **User Preferences**.
Wizard Map	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > **Affected Objects Page** > Review Summary Page > Summary Page.

The page includes the following element:

GUI Element	Description
<Affected Objects tree>	The Affected Objects tree includes all objects that are matched against the various filter criteria selected in the previous pages of the wizard. Select or clear objects as required for the replace operation. **Note**: When using Global Replace from System Availability Management Administration, a tree is displayed for each SiteScope selected.

Review Summary Page

Description	Use the Review Summary page to preview the objects on which the replacement operation is performed. The number of objects affected by the global replacement is given above the table listing the replacements. When working with multiple SiteScopes in System Availability Management Administration, a table is displayed for each SiteScope and the name of the SiteScope appears above the table.
Important Information	The number of objects that are affected by the global replacement is displayed above the table. Each table column can be sorted in ascending or descending order by right-clicking the column title. An up or down arrow indicates the sort order. Once you click **Finish** in this page, you cannot undo the replacement operation.
Wizard Map	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > **Review Summary Page** > Summary Page.

The page includes the following elements:

GUI Element	Description
▼ ▲	Change the sort order in the columns by clicking the up and down arrow in the column title. **Default:** The **Monitor Full Name** column is in alphabetical order, from top to bottom.
Monitor Full Name	The name format is <group name>/<monitor name>.
Property	The field name that you marked in the Choose Changes page that changes as a result of the replace operation.
Previous Value	The current value that changes as a result of the replace operation.
New Value	The new value that you entered in the Choose Changes page.

Summary Page

Description	The Summary page reports the changes that were implemented successfully and those in which errors occurred. The page displays the changes in table format. When working with multiple SiteScopes in System Availability Management Administration, a table is displayed for each SiteScope and the name of the SiteScope appears at the top of the table.
Important Information	The number of objects affected by the global replacement is given above the table. Each table column can be sorted in ascending or descending order by right-clicking the column title. An up or down arrow indicates the sort order. There is no way to undo changes made by the replace operation.
Wizard Map	The Global Search and Replace wizard includes: Select SiteScope Page (when working in System Availability Management Admin) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > Review Summary Page > **Summary Page**.

The page includes the following element:

GUI Element	Description
▼ ▲	Change the sort order in the columns by clicking the up and down arrow in the column title. **Default:** The **Monitor Full Name** column is in alphabetical order, from top to bottom.
Monitor Full Name	The name format is <group name>/<monitor name>.

GUI Element	Description
Property	The field name that you marked in the Choose Changes page that changed as a result of the replace operation.
New Value	The new value that resulted from the global replace operation.
🖨	Click to open a printer friendly version of the results. **Note**: This option is available only to users accessing Global Search and Replace from System Availability Management Administration.
OK	Closes the wizard. You return to System Availability Management Administration in Business Availability Center or SiteScope Dashboard in standalone.

16

Monitoring SiteScope Server Health

For reliability of operations monitoring depends in part on the reliability of the monitoring application. SiteScope can monitor several key aspects of its own environment to help uncover monitor configuration problems as well as SiteScope server load. Optionally, SiteScope can also monitor its connectivity and related data events when connected to HP Business Availability Center.

About the SiteScope Health Group

SiteScope Health is a specially designed group of monitors that display information about SiteScope's own health. This includes monitoring server resource usage, key processes, monitor load, and the integrity of key configuration files used by SiteScope. SiteScope Health monitoring data is also recorded in the daily monitor logs, by default, so you can create reports on SiteScope Health performance.

The Health monitor group is displayed as a special health icon within the main SiteScope container. You view the contents of the Health monitor group by clicking the **Health** container.

SiteScope Health monitoring includes special monitor types. These types include:

Monitor Type	Default Name	Description
Log Event Health Monitor	Log Event Checker	Checks for certain events logged to the SiteScope error log.
Monitor Load Monitor	Monitor Load Checker	Checks for data about the number of monitors being run or waiting to run.
Health of SiteScope Server Monitor	Health of SiteScope Server	Checks a large number of server process and resources for the server on which SiteScope is running.

See "SiteScope Health Monitor Reference" on page 299 for more information about the configuration of the individual SiteScope Health Monitors.

As with other SiteScope monitors and groups, you may associate alerts and reports with individual Health monitors to be notified of problems and review SiteScope performance over time.

Deploy SiteScope Health Monitors

SiteScope Health monitors are enabled automatically when SiteScope is deployed. This means that the monitors are normally present when you import a SiteScope to System Availability Management in HP Business Availability Center. If it is necessary to add SiteScope Health monitors to a SiteScope installation, you use a Health Template available in the monitor tree. The special monitor templates are deployed into the Health monitor group of the SiteScope you want to monitor. You use the following steps to deploy a set of SiteScope Health monitors.

To deploy SiteScope Health Monitors:

1 Open the SiteScope container to which you want to display the Health Monitors. Confirm that the SiteScope includes the Health monitor group container.

Note: The Health monitor group container is identified with a special health indicator icon.

---

2 Find the **Health Templates** in the monitor tree. Click to expand the container contents. The available Health monitor templates are displayed.

3 Select the Health monitor template for the operating system on which the SiteScope you want to monitor is running. The choices are:

- UNIX Health Monitors
- Windows Health Monitors

4 Right-click the template icon and select **Copy** from the action menu.

5 Right-click the **Health** monitor group container of the SiteScope to which you want to deploy the Health monitors and select **Paste** from the Action menu. The monitors in the selected template are then configured and deployed to the selected SiteScope server.

Understanding SiteScope Health Monitoring

This section contains information about how to interpret the results of SiteScope Health Monitoring and some actions to take if errors are detected. For more details on the specific SiteScope Health monitor measurements, see Chapter 17, "SiteScope Health Monitor Reference."

This section includes the following topics:

- "SiteScope Log Events" on page 296
- "SiteScope Monitor Load" on page 298
- "SiteScope Server Health" on page 298

SiteScope Log Events

The Log Event Monitor is the equivalent of a SiteScope monitor group that watches the SiteScope Error Log (error.log) for certain events. These events include Log entries indicating that a monitor has been skipped or there was a problem in reporting data to another application.

A SiteScope monitor is reported as skipped if the monitor fails to complete its actions before it is scheduled to run again. This can occur with monitors that have complex actions to perform, such as querying databases, stepping through multi-page URL sequences, waiting for scripts to run, or waiting for an application that has hung. This can also happen if there are too many monitors waiting to run that require a process from the process pool.

For example, assume you have a URL Sequence Monitor that is configured to transit a series of eight Web pages. This sequence includes performing a search which may have a slow response time. The monitor is set to run once every 60 seconds. When the system is responding well, the monitor can run to completion in 45 seconds. However, at times, the search request takes longer and then it takes up to 90 seconds to complete the transaction. In this case, the monitor has not completed before SiteScope is scheduled to run the monitor again. SiteScope detects this and makes a log event in the SiteScope error log. The SiteScope Log Event Monitor detects this and signals an error status.

A monitor may also skip if it is a monitor type that requires a process from the process pool but the process pool limit has been reached. Generally, this is not likely to happen but may occur in some situations with high monitoring load. The SiteScope Health Log Event Monitor also watches for process pool events.

Skipped monitors cause a number of problems. One is the loss of data when a monitor run is suspended due because a previous run has not completed or has become hung by a unresponsive application. Skipped monitors can also cause SiteScope to automatically stop and restart itself, an event that is also monitored by the SiteScope Health Log Event Monitor. A restart is done in an effort to clear problems and reset monitors. However, this can also lead to gaps in monitoring coverage and data. Adjusting the run frequency (**Frequency**) at which a monitor is set to run or specifying an applicable timeout value can often correct the problem of skipping monitors. Investigation of unresponsive systems that are being monitored may also be necessary.

Note:

- A **Max Monitor Skipping** setting has been added to allow monitors that are skipping to be disabled automatically. If this occurs, SiteScope is not restarted but an e-mail is sent to the SiteScope administrator about the skipping monitor to signal the disable event. This optional functionality is disabled by default but can be enabled by changing **Shutdown on monitor skips** to **true** in the Infrastructure Settings Preferences page. To access this page, expand **Preferences** in the left menu tree, choose **Infrastructure Settings Preferences**, and select the **Server Settings** section.
- You can control the maximum number of processes available from the **Maximum processes per pool** field in the Infrastructure Settings Preferences page. The default is 50. You should only change this setting if adjustments to monitor configurations do not resolve the monitor performance problems. To access this setting, expand **Preferences** in the left menu tree, choose **Infrastructure Settings Preferences**, and select the **General Settings** section.

The Log Event Monitor is also configured to report log events that indicate a problem with the transfer of SiteScope monitor and configuration data to an HP Business Availability Center installation. See the section on Integration with HP Business Availability Center for more information on Troubleshooting Data Reporting to Business Availability Center.

SiteScope Monitor Load

The Monitor Load Monitor is the equivalent of a SiteScope monitor group that watches how many monitors are running and how many are waiting to be run. Watching monitor load is important to help maintain monitoring performance and continuity. If the number monitors waiting approaches or exceeds the number of monitors running, adjustments should be made to monitor configurations to reduce the number of monitors waiting to run. Generally, this can be done by reducing the run frequency of some monitors.

SiteScope Server Health

The Health of SiteScope Server Monitor is the equivalent of a SiteScope monitor group that monitors server resources on the server where SiteScope is running. This includes monitors for CPU, disk space, memory, and key processes. A problem with resource usage on the SiteScope server may be caused by monitors with configuration problems or may simply indicate that a particular SiteScope is reaching it performance capacity. For example, high CPU usage by SiteScope may indicate that the total number of monitors being run is reaching a limit. High disk space usage may indicate that the SiteScope monitor data logs are about to exceed the capacity of the local disk drives (see the section on “Log Preferences” on page 250 for SiteScope data logging options).

17

SiteScope Health Monitor Reference

SiteScope Health Monitors are deployed by using the Health group page. The error, warning, and good status thresholds for these monitors are set in the same way as for other monitor types.

Log Event Health Monitor

This monitor is designed to check the **error.log** file for the local SiteScope installation. You can edit the counters, the update frequency and the display name for this monitor type in the Main Settings. You can use the Advanced Settings to disable the monitor individually as well as selecting other options as shown on the monitor properties panel.

The status thresholds for this monitor are based on the counters selected. The counters for this monitor type are listed in the table below.

Note: Only the first 15 selected counters are configured and monitored. A maximum of 10 measurements can be used as status threshold criteria for alerting.

Log Event Monitor Counters

The following table lists all the available counters for this health monitor:

Counter	Description
skipped #1	A monitor has skipped its scheduled run once.
skipped #2	A monitor has skipped its scheduled run two times.
skipped #3	A monitor has skipped its scheduled run three times.
skipped #4	A monitor has skipped its scheduled run four times.
skipped #5	A monitor has skipped its scheduled run five times.
SiteScope shutting down	SiteScope has been shut down.
Reached the limit of processes in the process pool	The number of processes requested from the process pool exceeds the number of processes available in the pool.
Error. data reporter failed to report chunk of data	There was a fault in the transfer of SiteScope monitor measurement data to HP Business Availability Center.
Error. config reporter failed to report chunk of data	There was a fault in the transfer of SiteScope configuration data to HP Business Availability Center System Availability Management.
Error. Topaz failed to process data	HP Business Availability Center reported a fault in processing data sent from SiteScope.
Error. CacheSender. Got to the max number of cached files	SiteScope has reached the maximum number of cached data file awaiting transfer to HP Business Availability Center. This may occur if data transfer between SiteScope and HP Business Availability Center has been interrupted.

Counter	Description
Error. CacheSender. Got to the max old dir size	SiteScope has reached the maximum directory size for cached data file awaiting transfer to HP Business Availability Center. This may occur if data transfer between SiteScope and HP Business Availability Center has been interrupted.
Topaz SEVERE	HP Business Availability Center reported a data transfer or processing fault with a status of SEVERE.

Status thresholds for this monitor are set on counters listed in the table above.

Monitor Load Monitor

This monitor is designed to check several SiteScope load statistics reported by the Progress Report for the local SiteScope installation. You can edit the counters, the update frequency and the display name for this monitor type in the Main Settings. You can use the Advanced Settings disable the monitor individually as well as selecting other options as shown on the monitor properties panel.

The status thresholds for this monitor are based on the counters selected. The counters for this monitor type are listed below.

Note: Only the first 15 selected counters are configured and monitored. A maximum of 10 measurements can be used as status threshold criteria for alerting.

The following counters are used for monitoring load:

- Current Monitors Run Per Minute
- Current Monitors Running
- Current Monitors Waiting
- Maximum Monitors Run Per Minute
- Maximum Monitors Running
- Maximum Monitors Waiting

Health of SiteScope Server Monitor

This monitor is designed to check the SiteScope server resource and process statistics for the local SiteScope installation. You can edit the counters, the update frequency, and the display name for this monitor type in the Main Settings. You can use the Advanced Settings to disable the monitor individually as well as selecting other options as shown on the monitor properties panel.

The status thresholds for this monitor are based on the counters selected. The counters available depend on the platform on which SiteScope is running. The counters for this monitor type are listed below.

Note: Only the first 15 selected counters are configured and monitored. A maximum of 10 measurements can be used as status threshold criteria for alerting.

Health of SiteScope Server Counters on UNIX

The following are default Health of SiteScope Server Monitor counters for SiteScope on UNIX platforms:

- Used Disk Space on SiteScope Drive
- MegaBytes Available on SiteScope Drive
- Used Disk Space on /
- MegaBytes Available on /
- Disk Blocks Written/sec
- Disk Blocks Read/sec
- Physical Memory Free
- Physical Memory Free Megabytes
- Swap Free,Swap Free Megabytes
- Load Avg 5min
- SiteScope Process Memory
- SiteScope Process Thread Count
- SiteScope Process Handle Count
- Average CPU
- PageIns/sec
- PageOuts/sec
- SwapIns/sec
- SwapOuts/sec
- ContextSwitches/sec
- Net_TotalPacketsIn/sec
- Net_TotalPacketsOut/sec
- Net_TotalCollisions/sec

Health of SiteScope Server Counters on Windows

On the Windows platform the counters for this monitor type are presented in an expandable tree selection menu. You use the navigation features to expand and collapse the selection menu and select counters to monitor. The following are default Health of SiteScope Server Monitor counters for SiteScope on Windows platforms:

System Component	Available Counters
skipped #1	A monitor has skipped its scheduled run once
Memory	Page Faults/sec Pool Paged Bytes Pool Nonpaged Bytes % Committed Bytes In Use Available MBytes
System	Context Switches/sec File Data Operations/sec System Up Time Processor Queue Length Processes Threads
Processor	_Total % Processor Time % DPC Time
Process	java Thread Count Pool Paged Bytes Pool Nonpaged Bytes Handle Count
Process	perfex % Processor Time Thread Count Pool Paged Bytes Pool Nonpaged Bytes Handle Count

System Component	**Available Counters**
Network Interface	MS TCP Loopback interface Bytes Total/sec Current Bandwidth Bytes Received/sec Bytes Sent/sec <*Ethernet_hardware*> (hardware specific to the particular SiteScope server) Bytes Total/sec Current Bandwidth Bytes Received/sec Bytes Sent/sec
LogicalDisk	<*logical_drive*> (hardware specific to the particular SiteScope server) % Free Space Free Megabytes Avg. Disk Bytes/Transfer _Total % Free Space Free Megabytes Avg. Disk Bytes/Transfer
PhysicalDisk	_Total Current Disk Queue Length Disk Transfers/sec <*physical_disk(s)*> (hardware specific to the particular SiteScope server) Current Disk Queue Length Disk Transfers/sec
Server	Bytes Total/sec Errors Logon Errors Access Permissions Errors System Files Open Server Sessions

18

Log Files

SiteScope maintains a number of log files that are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions.

Using Log Files

Log files can be accessed using the Log Files tab. The Log Files tab is available only on the **SiteScope** root node and for the **Health** node in the monitor tree.

The following table is an overview of the log files and their contents:

Log Name	Description
Alert Log	Records alert information whenever SiteScope generates an alert. This can be used to troubleshoot alert actions and to confirm that alerts were sent.
Error Log	Contains a variety of messages relating to the operation of SiteScope. This includes a record of errors that SiteScope may have encountered when trying to perform monitor actions or data communication actions. It also includes messages indicating when SiteScope was stopped or started and if there are monitors that are skipping because they are unable to complete their task.
Run Monitor Log	Records information when specific monitor runs and some actions related to managing monitors. This can be useful in troubleshooting monitors.
HP Business Availability Center Log	Contains information about connectivity and monitor data transfer when SiteScope is configured to report to HP Business Availability Center.
Post Log File	An optional log file used to record HTTP Post requests made to the SiteScope server. This can be used to track administrative actions performed. This log is only enabled when the _postLogFile=true setting exists in the master.config file.
URL Details	An optional log file used to record the complete contents of HTTP and HTTPS requests made by SiteScope URL monitor types. This can be used to troubleshoot URL and URL Sequence monitor types. This log is only enabled when the _urlDetailLogEnabled=true setting exists in the master.config file. This can be used selectively by adding the _urlDetailLogEnabled=true setting into an individual monitor group configuration file that contains a URL monitor type.

Log Name	Description
Operator Log	An optional log file used to record SiteScope operator actions, primarily information from use of the Acknowledgement feature. This log is created when an acknowledgement is added to one or more monitors.
Date Coded Monitor logs	This section contains links to the logs containing individual monitor measurements. SiteScope creates a new monitor log each day to record all monitors run during that 24 hour period. These logs are the basis for SiteScope Reports. **Note:** The monitor logs can become very large depending on the monitor environment. This may make it impractical to view them using a Web browser.
Audit Log	This section contains links to the logs containing all configuration changes that were performed, such as creation of monitors, templates, alerts and so on. For for information about audit logs, refer to "Audit Log" on page 317.

The log files are written in plain text and stored in the <**SiteScope_root_path**>**SiteScope****logs** directory.

You use the following steps to view SiteScope logs.

To view SiteScope logs:

1 Click the **SiteScope** node in the monitor tree. Alternatively, you can click on the **Health** container in the monitor tree. The applicable view is displayed.

2 Click the **Log Files** tab in the upper right area of the contents area. The Log Files page opens.

3 Click on the name of the log file you want to view. A new browser window opens displaying the text of the log file. You can use the scroll bars to view the contents of the log or use the browser's text Find utility to locate specific information. For example, you can search for a unique text string that appears in a monitor's **Name** property to locate entries for a particular monitor instance.

SiteScope Log File Columns

When SiteScope runs a monitor instruction to test the availability of components in the infrastructure, the monitor results are written to data log files. In the default configuration, these log files are tab-delimited text files. Understanding the order and content of these files is useful for examining particular monitor results or for porting the SiteScope monitor results to another database.

The first six columns of each log entry in a SiteScope monitor data log are the same for each monitor type. The following table describes the content of these columns. As noted, the columns in each log file are written as tab-delimited text.

Common Data Log Columns

Column	Data in Column
1	Time and date the sample was recorded.
2	Category (for example, good, error, warning, nodata).
3	Monitor group name where the monitor defined (also called ownerID).
4	Monitor title text.
5	stateString (this is the status string that shows up on the Monitor Group Detail Page).
6	id:sample number (a unique ID for this monitor where group + id is a unique key for a monitor). The sample number is a unique sample number for that monitor.

After the first six columns of each log entry, the content of each column is specific for each monitor type.

19

SiteScope Progress Report

Monitoring the availability of systems and servers that deliver business-critical services to users and customers is the focus of SiteScope. Together with the SiteScope Health monitoring, the SiteScope Progress Report Page provides several key indicators you use to monitor the performance of the SiteScope application.

About the SiteScope Progress Report

The SiteScope Progress page provides an overview several key SiteScope server performance metrics. At the top of the page, the SiteScope monitoring load statistics are displayed. The table in the lower section of the page displays which SiteScope monitors are running, and which monitors have run recently, at what time, and what was the returned status. This page is updated every 20 seconds, so the information is always current.

The SiteScope Progress page can be accessed using the Progress tab. The Progress tab is available only for the **Health** container in the monitor tree.

Understanding Monitoring Load

Monitoring Load can be a key indicator of SiteScope scaling problems, monitor configuration problems, or network performance issues. The following is a brief explanation of the SiteScope monitor execution model and interpreting the Progress Report in the context of this model.

A SiteScope monitor instance is essential an instruction set that is to be executed by the SiteScope application on a regularly scheduled interval. While a monitor instance is defined, SiteScope queues the monitor for execution based on the run (update) frequency and schedule options. If the monitor instance is marked as disabled, it is still scheduled in the queue but the normal instructions are not executed.

As a Java-based application, SiteScope makes use of multi-threading to accomplish parallel execution of monitor tasks. Each monitor instance scheduled for execution is assigned a thread. Once it is assigned a thread, the monitor instance becomes a **Monitor Running**. It remains bound to the thread until the monitor execution instruction has either received a result or the timeout value, if applicable, has been reached.

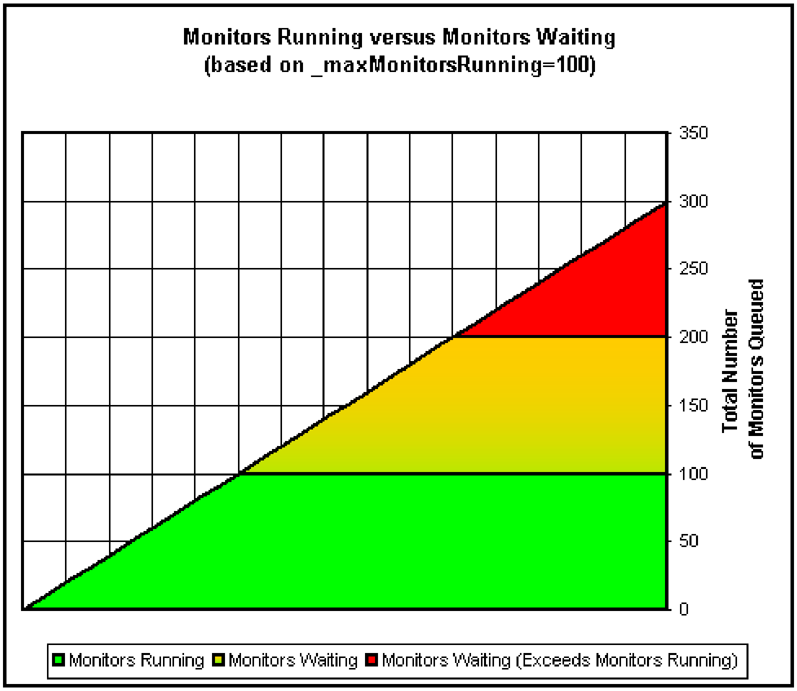
Even in this model, monitor execution is not instantaneous and there is a finite limit to the number of monitor threads that can be executed in parallel. If not more threads are available, a monitor that is queued for execution becomes a **Monitor Waiting** for an execution thread.

It is difficult to assign specific values and limits to SiteScope Monitoring Load because the specifics of the server capacity and network deployment can vary widely. The monitoring load may also vary significantly over time simply due to transient network traffic issues or SiteScope monitor configuration problems.

One key warning signal for interpreting monitoring load is the ratio of Monitors Waiting to Monitors Running. Generally, having some monitors waiting for execution is not a problem unless the ratio of Monitors Waiting to Monitors Running is consistently 1:2 or higher. For example, if the number of monitors running is at the maximum of 100 and there are 50 monitors waiting, this represents a ratio of 1 monitor waiting for every two running.

Note: The maximum number of monitor execution threads for monitors to run is controlled by the _maxMonitorsRunning=100 setting in the **master.config**.

The graph below presents a visualization of the relationship between Monitors Running and Monitors Waiting. This graph is based on the default _maxMonitorsRunning setting of 100 monitors. The green region shows that SiteScope is able to run all queued monitors until the number of queued monitors exceeds 100. At that level, additional monitors that are scheduled to run are given the status of Monitor Waiting. The red region represents an area where the number of monitors waiting is more than twice the number of monitors running. This is certain indication that your SiteScope monitor configurations are not well aligned with the capacity of the server and network.



You can adjust the following monitor configuration settings if there are consistently too many monitors waiting:

- **Update Every (frequency).** This is the basic schedule parameter for every monitor type. A large number of Monitors Running and Monitors Waiting can often be explained by a large number of monitors set to run (or update) at short intervals. The minimum update interval is 15 seconds. Depending on a number of system factors, there are several monitor actions which may take more than 15 seconds to complete. For example, Web transactions, database queries, logging onto remote servers, and some regular expression matches may delay monitor completion. Use the "Monitor Summary Report" on page 1273 to check the frequency setting for groups of monitors and consider increasing the value for some monitors.
- **Verify Error.** Regular or extensive use of this option has the effect of rapidly increasing the monitor run queue whenever the applicable SiteScope monitors detect an error condition. While this option has its purpose, it should not be used by default on every monitor. Use the "Monitor Summary Report" on page 1273 to list monitors that may have the Verify Error setting enabled.

Accessing the SiteScope Progress Report Page

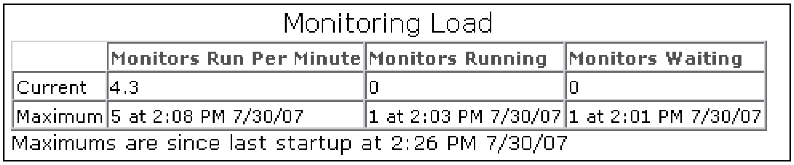
The Progress Report page contains the Load Measurements table that displays the load on the SiteScope server and the Recent Monitors table that lists the monitors that have most recently run by SiteScope.

To access the SiteScope Progress Report page:

1. Click the **Health** container in the monitor tree. The Progress tab is displayed at the top of the SiteScope Health page in the right pane.
2. Click the **Progress** tab. The SiteScope Progress Report opens.

The Monitoring Load Table

The Monitoring Load table is an important indicator of SiteScope performance. The following is a sample monitoring load table.



Monitoring Load

	Monitors Run Per Minute	Monitors Running	Monitors Waiting
Current	4.3	0	0
Maximum	5 at 2:08 PM 7/30/07	1 at 2:03 PM 7/30/07	1 at 2:01 PM 7/30/07

Maximums are since last startup at 2:26 PM 7/30/07

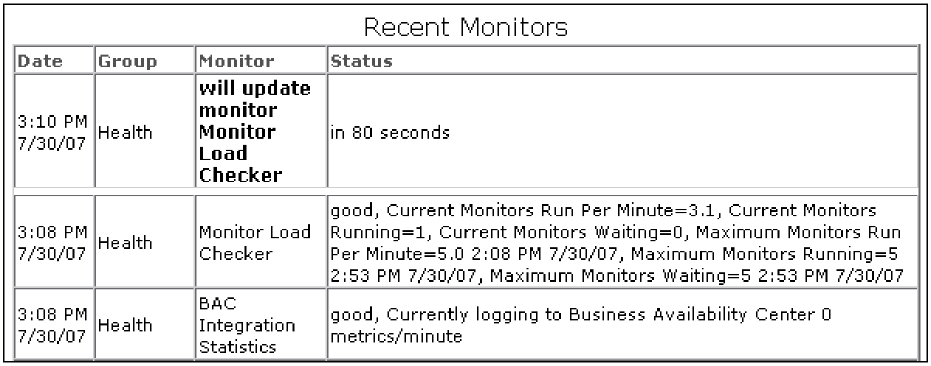
The following is an explanation of the data shown in the report table. Individually and taken together, these measurements are the primary measure of how heavily loaded the SiteScope server is as currently configured. For each statistic, the current and maximum values are displayed.

Parameter	Description
Monitors Run Per Minute	This is a rolling average of the last 10 minutes of monitoring, and tracks the rate (per minute) at which monitors are being run.
Monitors Running	This number represents the number of monitors queued for execution, based on their update frequency or schedule, that currently have execution threads. This means they are being executed.
Monitors Waiting	This measurement is the complement of the Monitors Running measurement representing the number of monitors queued for execution, based on their update frequency or schedule, that currently are awaiting execution threads. This means they are not being executed.

The Recent Monitors Table

Below the monitoring load table is the list of recent monitors run by SiteScope. The table is divided into two subsections with a simple blank row dividing the two sections. The first monitors in the list are displayed in bold text and indicate monitors that are currently being executed. The monitors displayed below the blank row divider are displayed in plain text and indicate the monitors that have most recently completed execution. The Progress Report page is automatically updated every 20 seconds

The following is a sample Recent Monitors table.



Recent Monitors

Date	Group	Monitor	Status
3:10 PM 7/30/07	Health	**will update monitor Monitor Load Checker**	in 80 seconds
3:08 PM 7/30/07	Health	Monitor Load Checker	good, Current Monitors Run Per Minute=3.1, Current Monitors Running=1, Current Monitors Waiting=0, Maximum Monitors Run Per Minute=5.0 2:08 PM 7/30/07, Maximum Monitors Running=5 2:53 PM 7/30/07, Maximum Monitors Waiting=5 2:53 PM 7/30/07
3:08 PM 7/30/07	Health	BAC Integration Statistics	good, Currently logging to Business Availability Center 0 metrics/minute

In this example, only one monitor instance, the **Monitor Load Checker** monitor instance, is being executed. The information in each column of the Recent Monitors table is described as follows:

Parameter	Description
Date	The date and time the monitor ran.
Group	The group to which the monitor belongs.
Monitor	The name of the monitor that SiteScope ran.
Status	The status returned by the monitor.

20

Audit Log

SiteScope's audit log contains configuration changes performed in the new user interface, such as creation of monitors, templates, alerts, and so forth.

Note: When SiteScope is attached to Monitor Administration in HP Business Availability Center, the actions you perform on SiteScope appear in HP Business Availability Center's audit log and not in SiteScope's audit log.

About the Audit Log

The audit log provides you with a record of actions performed in SiteScope, the time they were performed, and by whom. As each operation is performed, an entry is made in the audit log. When the current audit log reaches its size limit, it is closed and a new log is created. For details, see "Configuring the Audit Log" on page 318.

Most operations performed in the monitor tree are recorded in the audit log. For a list of exceptions, see "Audit Log Troubleshooting and Limitations" on page 331.

Configuring the Audit Log

The maximum size of the audit log is determined by the parameters in: **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties**:

- **MaxFileSize.** The maximum number of lines in the log.
- **MaxBackupIndex.** The maximum number of backup audit logs to be kept before the oldest audit log is deleted.

  For example, if **MaxBackupIndex** is 5, no more than 5 backup audit logs are kept. If 5 backup log files exist, then after the current audit.log file reaches **MaxFileSize** size, audit.log.5 is deleted, audit.log.4 is renamed to audit.log.5, audit.log.3 to audit.log.4 and so forth. The current audit.log is renamed audit.log.1 and a new audit.log is created.

Accessing the Audit Log

The audit log is found in the <**SiteScope root directory**>**SiteScope****logs** directory. You can access it from the directory or through the SiteScope application as described below.

The name of the current audit log is **audit.log**. Older logs are named audit.log.1, audit.log.2, and so forth. The higher the number concatenated to the name, the older the log.

To check user privileges to view the audit log:

1. In the monitor tree, select **User Preferences** and click the user name.
2. In the contents page, open the **Other Options** pane. If **View Logs** check box is not checked, click **Edit**, and then check the **View Logs** check box.
3. Click **OK** to save your change and exit. Click **Cancel** to exit without saving your change.

To view the audit log:

1. In the monitor tree, click the **SiteScope** node or the **Health** container.
2. In the upper-right area of the contents page, click the **Log Files** tab. The Logs page opens.
3. Click the **Audit Log** link. A Web browser window with audit log entries opens.

   Use the scroll bar or your Web browser's **Find** utility to locate specific information on the page.

   If there is more than one audit log, search for the required records in one of the backup audit logs.

Audit Log Entries

Each line of the audit log describes an operation performed in SiteScope.

This section includes the following:

SiteScope Startup

When SiteScope is restarted, its entry is:

```
YYYY-MM-DD HH:MM:SS - SiteScope Audit Log initialized
```

Group Operations

Operations performed on groups have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Group
‘<group_name>’ ‘<operation>’ ‘<container>’
```

where:

- <**group_name**> is the name of the group that was operated on.
- <**operation**> can be one of the following:
  - **Created In.** The location where the group was created.
  - **Updated in.** The location where the group’s information was updated.
  - **Deleted From.** The location from where the group was deleted.
  - **Pasted On.** The user copied information from one group to another.
- <**container**> is the name of the group container that was operated on.

Monitor Operations

Operations performed on monitors have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Monitor
‘<monitor_name>’ ‘<operation>’ ’<container>’
```

- <**monitor_name**> is the name of the monitor that was operated on.
- <**operation**> can be one of the following:
  - **Created In.** The location where the user created a monitor.
  - **Updated in.** The location from where the user updated a monitor’s information.
  - **Deleted From.** The location where the user deleted a monitor.
  - **Pasted On.** The user copied information from one monitor to another.
- <**container**> is the name of the container.

Update to General Preferences

Changes made in **General Preferences** under the **Preferences** container in the monitor tree have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed:
‘<preferences_name>’ updated
```

where <**preferences_name**> is the name of the preference that was changed.

The nature of the change to the preference is not in the log.

Update to Other Preferences

Changes to preferences other than those listed in **General Preferences** in the monitor tree have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed:
‘<preferences_name>’ named ‘<object_name>’ ‘<operation>’
```

- <**preferences_name**> is the name of the preference.
- <**object_name**> is the name of the object to which the preference refers.
- <**operation**> can be one of the following:
  - **Updated.** The user changed the preference.
  - **Deleted.** The user deleted the preference.

This format is used for the following types of preferences:

- Windows Remote Preferences
- UNIX Remote Preferences
- Mail Preferences
- Pager Preferences
- SNMP Preferences
- Absolute Schedule Preferences
- Range Schedule Preferences
- User Preferences
- Dynamic Update Preferences

Applying Templates

When an entity is created by deploying a template, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Configuration
Template ‘<template_name>’ pasted on ‘<group_name>’
```

- <**template_name**> is the name of the template from which the entity was created.
- <**group_name**> is the name of the group that contains the entity that was created from the template.

Note: To see which entities were created by deploying the template, look at the contents of template itself. Information about entities is not included in the audit log.

Template Containers

When a template container is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
Container ‘<container_name>’ ‘<operation>’ ‘<container>’
```

- <**container_name**> is the name of the template container that was either created, deleted, or updated.
- <**operation**> can be one of the following:
  - **Created in.** The location where the user created the template container.
  - **Deleted from.** The location from where the user deleted the template container.
  - **Updated in.** The location where the user changed the template container.
- <**container**> is the name of the container containing the template.

Create, Delete, Modify Templates

When a template is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
‘<template_name>’ ‘<operation>’ ‘<container>’
```

- **<template_name>** is the name of the template that was either created, deleted, or updated.
- **<operation>** can be one of the following:
  - **Created in.** The location where the user created the template.
  - **Deleted from.** The location from where the user deleted the template.
  - **Updated in.** The location where the user changed the template.
- **<container>** is the name of the container containing the template.

Template Variables

When a template variable related to an object, such as server ID, is created, deleted, or updated in a container, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
Variable ‘<variable_name>’ ‘<operation>’ ‘<container>’
```

- **<variable_name>** is the name of the variable that was either created, deleted, or updated.
- **<operation>** can be one of the following:
  - **Created in.** The location where the template variable for the object was created.
  - **Deleted from.** The location where the template variable for the object was deleted.
  - **Updated in.** The location where the template variable for the object was updated.
- **<container>** is the name of the container containing the template variable.

Template Groups

When a template group for a specific type of object is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template Group
‘<group_name>’ ‘<operation>’ ‘<container>’
```

- <**group_name**> is the name of the template group created, updated or deleted.
- <**operation**> can be one of the following:
  - **Created in.** The location where the template group for the object was created.
  - **Deleted from.** The location from where the template group for the object was deleted.
  - **Updated in.** The location where template for the object was updated.
- <**container**> is the name of the container containing the template group.

Template Remote Objects

When a template remote server is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
Remote ‘<remote_name>’ ‘<operation>’ ‘<container>’
```

- <**remote_name**> is the name of the remote server.
- <**operation**> can be one of the following:
  - **Created in.** The location where the remote entity was created.
  - **Deleted from.** The location from where the remote entity was deleted.
  - **Updated in.** The location where the remote entity was updated.
- <**container**> is the name of the container containing the remote entity.

Template Alerts

When a template for an alert is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template Alert
‘<alert_name>’ ‘<operation>’ ‘<container>’
```

- <**alert_name**> is the name of the object for which the template alert is defined.
- <**operation**> can be one of the following:
  - **Created in.** The location where the template alert was created.
  - **Deleted from.** The location from where the template alert was deleted.
  - **Updated in.** The location where the template alert was updated.
- <**container**> is the name of the template container.

Template Monitors

When a template for a monitor is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
‘<monitor_name>’ ‘<operation>’ ‘<container>’
```

- <**monitor_name**> is the name of the monitor.
- <**operation**> can be one of the following:
  - **Created in.** The location where the template for the monitor was created.
  - **Deleted from.** The location from where the template for the monitor was deleted.
  - **Updated in.** The location where the template for the monitor was updated.
- <**container**> is the name of the container containing the template.

Alerts

Operations performed on alerts are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Alert
‘<alert_name>’ ‘<operation>’ ’<container>’
```

- <**alert_name**> is the name of the alert.
- <**operation**> can be one of the following:
  - **Created In.** The location where the new alert was created.
  - **Updated in.** The location where the new alert was updated.
  - **Deleted From.** The location from where the new alert was deleted.
  - **Pasted On.** The user copied information from one alert to another.
- <**container** > is the container of the alert.

Reports

Operations performed on report definitions are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Report
‘<report_name>’ ‘<operation>’ ’<container>’
```

- <**report_name**> is the name of the report.
- <**operation**> can be one of the following:
  - **Created In.** The location where a new report was created.
  - **Updated in.** The location where a new report was updated.
  - **Deleted From.** The location from where a new report was deleted.
  - **Pasted On.** The information was copied from one report to another.
- <**container** >. The container of the report.

Global Search and Replace Operations

Global Search and Replace operations are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: GSAR operation
started
-----------------------------------------------------------------------------------------------
YYYY-MM-DD HH:MM:SS -Global Replace updated group ‘<group_name>’
YYYY-MM-DD HH:MM:SS -Global Replace updated report ‘<report_name>’
YYYY-MM-DD HH:MM:SS -Global Replace updated monitor ‘<monitor_name>’
YYYY-MM-DD HH:MM:SS -Global Replace updated alert ‘<alert_name>’
YYYY-MM-DD HH:MM:SS -Global Replace updated preference ‘<preference_name>’
-----------------------------------------------------------------------------------------------
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: GSAR operation
finished
```

Start and end operations always appear in the log. The entries appear depending on the actions performed by the Global Search and Replace.

Login-Logout

Login and logout are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: <message>
```

where <**message**> is either:

- Logged in.
- Logged out.

Failed Login

Failed login attempts are in the format:

```
YYYY-MM-DD HH:MM:SS - Username and password do not match. Failed to login.
```

Changed Password

Password operations are logged and appear in the following format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: <message>
```

where <**message**> is either:

- Changed password successfully.
- Failed to change password.

Categories

Operations performed on categories are logged and appear in the following format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Category
‘<category_name>’ ‘<operation>’
```

- <**category_name**> is the name of the category.
- <**operation**> can be one of the following:
  - **Created.** The location where a new category was created.
  - **Updated.** The location where a new category was updated.
  - **Deleted.** The location from where a new category was deleted.

Audit Log Troubleshooting and Limitations

- Audit log entries can only be created in English. This means that audit log entries are also displayed only in English, regardless of what language you use to view SiteScope.
- The following operations are not recorded in the audit log:
  - When a template is deployed, operations on the various elements in the template are not logged.

    For example, you deployed a template that created group MM2_Servers with monitors in the new group. The audit log entry is:

    ```
    Operation performed: Configuration Template 'MM2' pasted on
    ‘MM2_Servers’.
    ```

    Note that there are no entries in the audit log about creation of monitors in MM2_Servers group.
  - Attaching and detaching SiteScope to HP Business Availability Center are not logged.

    When SiteScope is attached to Monitor Administration in HP Business Availability Center, the actions you perform on SiteScope appear in HP Business Availability Center’s audit log and not in SiteScope’s audit log.
  - Group configurations that were made by using a <group name>.mg file are not recorded in the audit log. Only group changes made through the monitor tree are recorded in the audit log.

    When you create a group in the monitor tree, a <group name>.mg file with all the configuration changes for the group is automatically created for that group. This means that you can configure a group through the monitor tree or by changing its mg file.

Part III

SiteScope Dashboard

21

SiteScope Dashboard Concepts and Tasks

This chapter includes the main concepts, tasks and reference information for SiteScope Dashboard.

Overview of SiteScope Dashboard

SiteScope monitoring provides a real-time picture of system availability and performance. You configure SiteScope monitors to collect metrics from a range of infrastructure components, including Web, application, database, and firewall servers. The status and metrics are then aggregated for presentation in SiteScope Dashboard.

Dashboard is linked to the SiteScope monitor tree hierarchy. The data displayed in Dashboard represents the selected context in the monitor tree. The highest level is the SiteScope node and any applicable monitor groups. The lowest-level element for display in a Dashboard view is an individual SiteScope monitor and its measurements.

Dashboard includes features that you can use to customize the display of monitor information. This includes defining named filter settings to limit the display of data to those matching a defined criteria. You can also select various data display options.

Dashboard also includes hyperlinks and menus that you can use to navigate through the hierarchy of monitor elements, manually run a monitor, disable monitors, and access alert definitions.

Overview of Dashboard Filter

You can filter monitors or groups by the following criteria:

- monitor or group names containing a specific text string
- monitors or groups monitoring a specific host or server
- monitors or groups reporting an error
- measurement results containing a specific text string

Filters are applied primarily to monitors. The filter criteria are not applied to groups, alerts, or reports. You can use view settings to filter on other elements. For more information, see “Views and Categories” on page 171.

Filters are applied to all Dashboard views. This means that some monitors may not be displayed depending on the filter criteria and the selected node. Generally, it is best to use filters together with the **Show all descendent monitors** view option. Filters remain active until you change or reset the filter criteria in the Dashboard Filter window.

Dashboard filters are separate from SiteScope views. You can use either Dashboard filters or views to filter the display of nodes to specific monitor types. However, Dashboard filters are applied to the results of any currently selected view setting. If a view setting is active, this may prevent the Dashboard filter from finding monitors that match the filter criteria, even if such monitors do exist in the SiteScope environment.

You can save a filter setting by defining the filter settings and then saving the view as a Dashboard Favorite. See the section "Defining and Managing View Settings" on page 172 for more information.

For details, see "Dashboard Filter Page" on page 352.

Generating a Server Centric Report

For Windows Resource Monitors and UNIX Resource Monitors, you can generate a Server Centric Report which displays data from three different metrics about the server being monitored. It is recommended to use Solution Templates when creating the Windows Resource Monitor or UNIX Resource Monitor. For details on the Solution Templates, see:

- "AIX Host Solution Templates" on page 1083
- "Linux Host Solution Templates" on page 1099
- "Solaris Host Solution Templates" on page 1149
- "Windows Host Solution Template" on page 1177

You can define the monitor manually by selecting **Enable Server Centric Report** in the appropriate monitor settings page, as described in "Windows Resources Monitor Settings" on page 833 and "UNIX Resources Monitor Settings" on page 818. When defining the monitor manually, you must select the required metrics for the monitors, according to the table in "Server Centric Report Measurements" on page 347.

The report displays the following metrics on the same graph:

- **CPU Utilization.** For UNIX Resource Monitors, this metric is calculated as an average of three counters: system processing utilization, user processing utilization, and input/output processing utilization. For Windows Resource Monitors, the metric is calculated as processing capacity used out of total processing capacity.
- **Memory Utilization.** Calculated as memory used out of total available memory.
- **Network Utilization.** Calculated by system-specific counters. Calculating network utilization is supported only for Windows servers.

Each metric is displayed by a separate line of a unique color on the graph. The report enables you to easily make a visible correlation between the different metrics.

The report also includes tables listing the top five processes by CPU utilization and memory consumption. You can navigate the graph and change the time of the data displayed in the tables. This enables you to focus in on a problematic period in the graph to locate the processes running at that time. For details on the Server Centric Report interface, see "Server Centric Report" on page 359.

Acknowledging Monitor Status

The acknowledgement feature can be used to track resolution of problems that SiteScope detects in your system and network infrastructure. With this feature, SiteScope keeps a record of when the problem was acknowledged, what actions have been taken, and by which user.

It also enables you to temporarily disable alerting on the monitors. This is useful to avoid redundant alerts while a problem is being actively addressed. You can also use the acknowledgement feature as a simple trouble ticket system when more than one person uses SiteScope to manage system availability.

Note: The acknowledgement feature is available only in Dashboard views. The acknowledgement icon is displayed only in Dashboard Detailed views.

You can add an acknowledgement to individual monitors or monitor groups. An acknowledgement added to a monitor applies only to that monitor. Any alert disable condition selected in the acknowledgement applies only to that monitor instance. Acknowledging a group applies the acknowledgement description and alert disable conditions to all monitors within the group. Acknowledgements applied to a group can be edited or deleted individually for monitors in the group.

Only one acknowledgement can be in force for a monitor or group at any given time. Acknowledgement comments and acknowledgement indicators continue to be displayed in the interface until they are deleted, even after any applicable alert disable schedule has expired.

Acknowledgement data and comments are written to a log file on the SiteScope machine. A new log entry is made each time you add, edit, or delete an acknowledgement. After a problem monitor is acknowledged, or the acknowledged status is cleared, you can view the history in the Acknowledge log. The Acknowledge Log for an item can be viewed even if there is no acknowledgment currently in force.

Accessing SiteScope Tools

SiteScope contains a number of tools that can be used to test the monitoring environment. You can use these tools to query the systems you are monitoring and view detailed results of the action. This may include simply testing network connectivity or verifying login authentication for accessing an external database or service. You can run these tools directly from the Dashboard group and monitor status information area by accessing the menu to the right of the **Name** column for the monitor or group.

For details on the different tools that are available, see “Working with SiteScope Tools” on page 1380.

Note: SiteScope Tools option is only available for individual monitors.

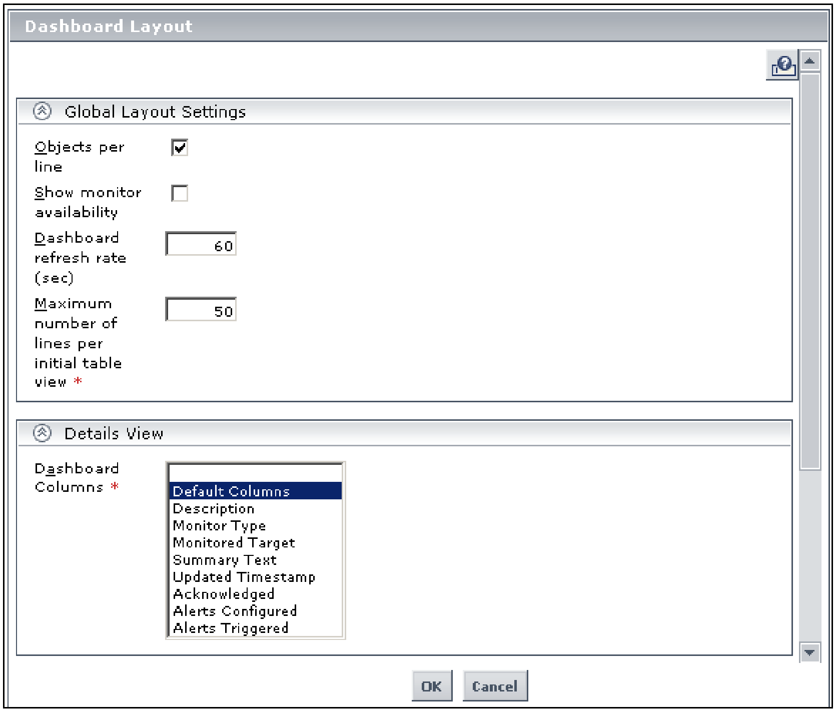
Customize SiteScope Dashboard

You can customize the display and content of SiteScope Dashboard by setting the layout and configuring filters.

Set the Dashboard Layout

Customize the display of group and monitor information using the settings on the Dashboard Layout page. For details, see “Dashboard Layout Page” on page 356.

Example



Dashboard Layout

Global Layout Settings

Objects per line ☑

Show monitor availability □

Dashboard refresh rate (sec) 60

Maximum number of lines per initial table view * 50

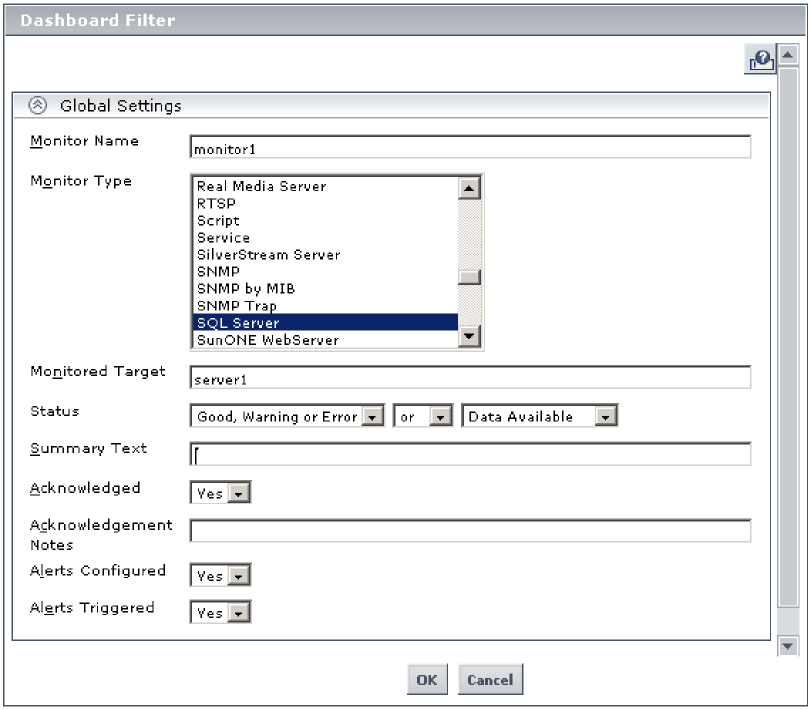
Details View

Dashboard Columns *
- Default Columns
- Description
- Monitor Type
- Monitored Target
- Summary Text
- Updated Timestamp
- Acknowledged
- Alerts Configured
- Alerts Triggered

Select and Set a Dashboard Filter

Configure and set a Dashboard filter by selecting from the options available on the Dashboard Filter page. For details, see “Dashboard Filter Page” on page 352.

Example



Monitor Name: monitor1

Monitor Type:
- Real Media Server
- RTSP
- Script
- Service
- SilverStream Server
- SNMP
- SNMP by MIB
- SNMP Trap
- SQL Server
- SunONE WebServer

Monitored Target: server1

Status: Good, Warning or Error | or | Data Available

Summary Text:

Acknowledged: Yes

Acknowledgement Notes:

Alerts Configured: Yes

Alerts Triggered: Yes

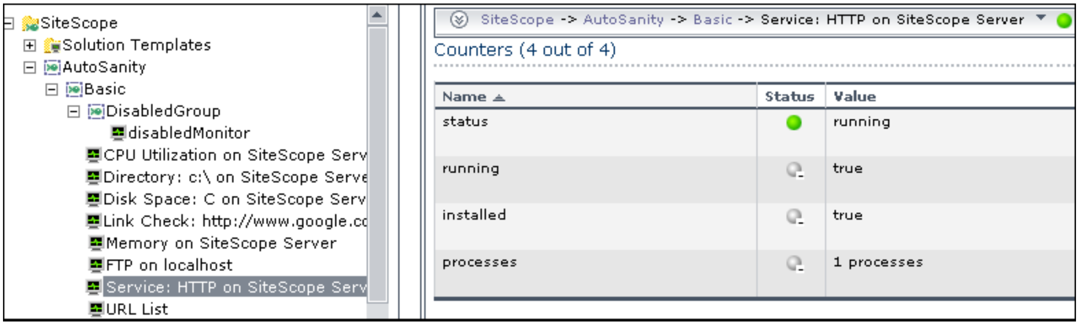
Analyze Data in SiteScope Dashboard

The following task describes the steps to follow to analyze data in SiteScope Dashboard.

Drill Down to View Monitor and Measurement Status and Availability

When viewing SiteScope data in the Current Status tab of Dashboard, you can drill down in the monitor tree to view monitor and measurement status and availability. For details on navigating in the Dashboard, see “SiteScope Dashboard - Current Status Tab” on page 363.

Example


SiteScope
Solution Templates
AutoSanity
Basic
DisabledGroup
disabledMonitor
CPU Utilization on SiteScope Serv
Directory: c:\ on SiteScope Serve
Disk Space: C on SiteScope Serv
Link Check: http://www.google.cc
Memory on SiteScope Server
FTP on localhost
Service: HTTP on SiteScope Serv
URL List

SiteScope -> AutoSanity -> Basic -> Service: HTTP on SiteScope Server ●

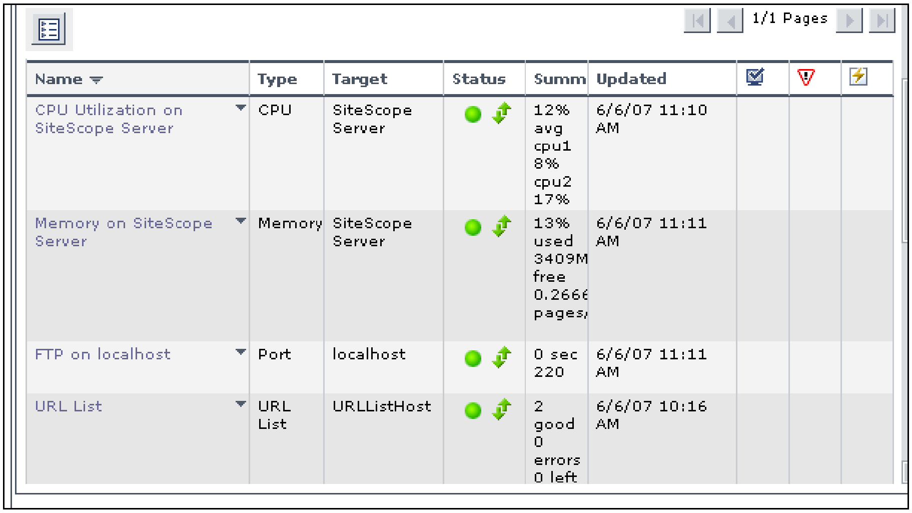
Counters (4 out of 4)

Name ▲	Status	Value
status	●	running
running		true
installed		true
processes		1 processes

View Configured and Triggered Alerts

You can view data about alerts in the configured alerts and triggered alerts columns. If no alerts are configured for a monitor, the alert columns do not appear. For details, see "SiteScope Dashboard - Current Status Tab" on page 363.

Example



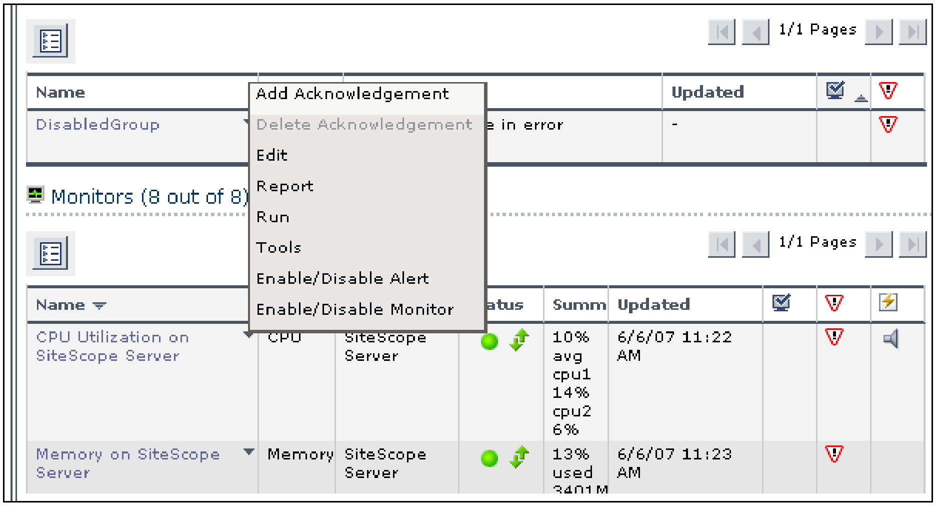
1/1 Pages

Name	Type	Target	Status	Summ	Updated	☑	▽	⚡
CPU Utilization on SiteScope Server	CPU	SiteScope Server	● ⇅	12% avg cpu1 8% cpu2 17%	6/6/07 11:10 AM			
Memory on SiteScope Server	Memory	SiteScope Server	● ⇅	13% used 3409M free 0.2666 pages/	6/6/07 11:11 AM			
FTP on localhost	Port	localhost	● ⇅	0 sec 220	6/6/07 11:11 AM			
URL List	URL List	URLListHost	● ⇅	2 good 0 errors 0 left	6/6/07 10:16 AM			

Acknowledge Monitors

To acknowledge monitor status, select Add Acknowledgement from the menu in the Name column, and fill in the Acknowledge dialog box. For details, see “Acknowledge Dialog Box” on page 350.

Example



Name		Updated
DisabledGroup	e in error	-

Name			atus	Summ	Updated
CPU Utilization on SiteScope Server	CPU	SiteScope Server	●	10% avg cpu1 14% cpu2 6%	6/6/07 11:22 AM
Memory on SiteScope Server	Memory	SiteScope Server	●	13% used 3401M	6/6/07 11:23 AM

View Monitor History

You configure monitor history in the General Preferences container, as described in “Dashboard Monitor History View Options” on page 231.To view monitor history, click the Monitor History tab in SiteScope Dashboard. For details on viewing monitor history data, see “SiteScope Dashboard - Monitor History Tab” on page 369.

Monitor Your Windows/UNIX Server's Resources

You can monitor your Windows or UNIX Server's resources by creating a Windows or UNIX Resource Monitor and generating a Server Centric report, as described in the following workflow:

Create a Windows/UNIX Resource Monitor

To monitor your Windows or UNIX Server, you must create a Windows Resource Monitor or UNIX Resource Monitor. It is recommended to do this using Solution Templates.

For details on the Solution Templates, see:

- "Windows Host Solution Template" on page 1177
- "AIX Host Solution Templates" on page 1083
- "Linux Host Solution Templates" on page 1099
- "Solaris Host Solution Templates" on page 1149

You can also create a Windows or UNIX Resource Monitor manually. For Windows Resource Monitors, see "Windows Resources Monitor Settings" on page 833. For UNIX Resource Monitors, see "UNIX Resources Monitor Settings" on page 818. Make sure to select **Enable Server Centric Report** and select the appropriate measurements. For details on the measurements, see "Server Centric Report Measurements" on page 347.

Generate the Server Centric Report

To monitor your server, navigate to Dashboard, display the data for the applicable Windows Resource or UNIX Resource monitor, and click the server name in the Target column in the row corresponding to your Windows or UNIX Resource monitor. The Server Centric Report opens.

Analyze Data in Report

The report enables you to view three different metrics of your server in the same graph – CPU utilization, memory utilization, and network utilization. It also lists the top five processes by CPU utilization and memory consumption. You can drill down to specific times by clicking a data point on the graph. For details, see "Server Centric Report" on page 359.

Server Centric Report Measurements

The following table displays the counters which must be selected when defining the monitor for the Server Centric Report manually:

OS Type	Server Centric Mandatory Counters
Counters for Windows Resource Monitor	Memory\% Committed Bytes In Use
	Processor_Total\% Processor Time
Counters for UNIX Resource Monitor on Solaris Platform	CPU utilization\%sys
	CPU utilization\%usr
	CPU utilization\%wio
	Memory\swap_avail
	Memory\swap_resv
Counters for UNIX Resource Monitor on AIX Platform	Processor\Total\%sys
	Processor\Total\%usr
	Processor\Total\%wio
Counters for UNIX Resource Monitor on Linux Platform	Memory\MemFree
	Memory\MemTotal
	Processor\Total\System
	Processor\Total\User
	Processor\Total\User low

For details on selecting counters for monitor definition, see “Windows Resources Monitor Settings” on page 833 (for Windows Resource Monitor counters) and “UNIX Resources Monitor Settings” on page 818 (for Solaris, AIX, and Linux platforms).

22

SiteScope Dashboard User Interface

This chapter includes a description of the pages and dialog boxes that are part of the SiteScope Dashboard user interface.

Acknowledge Dialog Box

Description	Enables you to add or edit an acknowledgement for a monitor. **To access:** Click the small black arrow in the **Name** column and select **Add Acknowledgement** from the menu (for groups).
Included in Tasks	"Analyze Data in SiteScope Dashboard" on page 343
Useful Links	"Acknowledging Monitor Status" on page 339

The Acknowledge dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Acknowledge Comment	Enter an acknowledgement comment which is displayed as a tooltip associated with the acknowledgement icon in the Dashboard view and is recorded in the Acknowledge Log. You can update the comment as new information becomes available. The comment is displayed until the acknowledgement is deleted.
Disable alerts for the next time period	Use this option to disable alerting immediately and to continue suppressing alerting on the selected monitor or group for a duration that you specify.
Disable Description	Enter an optional text description for alert icons associated with the monitors in the acknowledged context. The text description is added to the tool tip text that is displayed when the pointer is placed over any alert icon associated with the monitor in the Dashboard view. This text is displayed only while the alert disable option is in force. It is not written to the Acknowledge Log.
Disable on a one-time schedule	Use this option to disable alerting during a period of time that you specify. This can be useful if the system being monitored is expected to be unavailable during a certain period but you want to continue to run the monitor without triggering an alert.

GUI Element	Description
Undo one-time schedule	Cancel a one-time schedule disable alert.
View Acknowledge Log	View all acknowledgement entries for the group from which you invoke the acknowledgement dialog.

Add Dashboard Favorite Dialog Box

Description	Enables you to define combinations of Dashboard filter and layout settings (which were selected using the Dashboard Filter dialog box and the Dashboard Layout dialog box) and save them as a named favorite view. **To access:** Click the **Add Favorite** button in Dashboard.
Important Information	Dashboard favorites are limited to settings that are applicable to Dashboard views. This means that Dashboard favorites do not save user-global view settings, or the context that was selected in the monitor tree when the favorite was saved.
Included in Tasks	"Customize SiteScope Dashboard" on page 341
Useful Links	"Overview of SiteScope Dashboard" on page 336

The Add Dashboard Favorite dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Existing Favorites	A list of the existing favorite views. If you want to replace one of the existing favorites with the current settings, click on the favorite and it appears in the **Name** box.
Name	Enter a display name for the favorite view settings.

Delete Dashboard Favorites Dialog Box

Description	Enables you to delete existing favorite views. **To access:** Click the **Delete Favorites** button from Dashboard.
Included in Tasks	"Customize SiteScope Dashboard" on page 341
Useful Links	"Overview of SiteScope Dashboard" on page 336

The Delete Dashboard Favorites dialog box includes the following element:

GUI Element	Description
Existing Favorites	Select the view or views you want to delete from the list of current favorite views.

Dashboard Filter Page

Description	Enables you to configure a Dashboard filter by entering match criteria and selecting from the menu options. **To access:** Click the **View or edit filter** button in Dashboard.
Important Information	Any combination of filter options may be included in a single filter. For example, the filter definition can filter on a combination of **Monitor Type**, **Monitored Target**, and **Status**.
Included in Tasks	"Customize SiteScope Dashboard" on page 341
Useful Links	"Overview of Dashboard Filter" on page 336

The Global Settings area of the Dashboard Filter dialog box includes the following elements (listed alphabetically):

GUI Element	Description
?	Click the **Show Descriptions** button to display additional information about the dialog box elements.
Acknowledged	Use this option to filter monitors based on their Operator Acknowledgement status. To filter on monitors that have been acknowledged, select **Yes** from the drop-down menu. To filter on unacknowledged monitors, select **No** from the drop-down menu. **Note:** The Operator Acknowledgement feature is an optional interface functionality that is enabled using the SiteScope General Preferences.
Acknowledgement Notes	Use this option to filter monitors based on text that may appear in their Operator Acknowledgement notes. You can enter a literal text string or a regular expression to match a text pattern. For details about regular expressions see “Using Regular Expressions” on page 1281.
Alerts Configured	Use this option to filter monitors based on whether alerts have been configured on them. To filter on monitors that have one or more alerts configured on them, select **Yes** from the drop-down menu. To filter on monitors that do not have configured alerts, select **No** from the drop-down menu.
Alerts Triggered	Use this option to filter monitors based on whether they have triggered an alert event. To filter on monitors that have generated one or more alerts, select **Yes** from the drop-down menu. To filter on monitors that have not generated alerts, select **No** from the drop-down menu.
Monitored Target	Enter the server name to filter monitors based on a particular host or server being monitored.

GUI Element	Description
Monitor Name	Enter a text string or regular expression that matches the name of one of more monitors. When you apply this filter to the Dashboard view, only the monitors that match the **Monitor Name** criterion are displayed.
Monitor Type	Use this list to create a filter to display only selected monitor types.
Status	Use this option to filter monitors by reported status. The status filter criterion can be defined in terms of monitor category status. **Example:** Create a filter that displays only those monitors reporting a warning or error. The following status options are available: ➤ **Any Status.** Show all monitors with any status. This is the default option. This is can be used in combination with the **Data Available** option to filter out monitors that are in error due to connectivity or availability factors. ➤ **Good, Warning, or Error.** Show all monitors except those reported as disabled. ➤ **Error.** Show only monitors reporting an error status. ➤ **Warning or Error.** Show only monitors reporting a warning or error status. ➤ **Warning.** Show only monitors reporting a warning status. ➤ **Warning or Good.** Show only monitors reporting a warning or good status. ➤ **Good.** Show only monitors reporting a good or OK status. ➤ **Disabled.** Show only monitors reported as disabled.

GUI Element	Description
Status (with Availability)	Use this option to create a compound filter by combining the monitor status category with the data availability status. The following data availability status options are available: ➤ **Data Available.** Show monitors for which data is available, meaning the monitor was able to retrieve measurements from the target system. ➤ **Data Unavailable.** Show monitors for which data is not available, meaning SiteScope was not able to retrieve measurements from the target system. **Example:** Create a filter that displays only those monitors reporting **Error** and **Data Available**. This means that the filter shows monitors that indicate an error status for which the monitor was able to receive data from the monitored system as opposed to monitors that are reporting an error because the monitor was not able to communicate with the monitored system (that is, **Data Unavailable**).
Summary Text	Use this option to filter monitors based on text included in their summary string. You can enter a literal text string or a regular expression to match a text pattern. For details about regular expressions see "Using Regular Expressions" on page 1281.

The Monitor History Settings area of the Dashboard Filter dialog box includes the following elements (listed alphabetically):

GUI Element	Description
Display Time Period	Select the time frame for past events. **Default:** Past 1 hour
Monitor Runs per Screen	Enter the number of rows of data to display on the screen. **Default:** 100
Monitor Run Status	Select the appropriate event status, relational operator, and data availability.

Dashboard Layout Page

Description	You use the Dashboard Layout settings to customize the display of group and monitor data in the Dashboard views. This allows you to enable or suppress the display of monitor measurement details, alert information, and acknowledgement features. **To access:** Click the **View or edit layout** button in Dashboard.
Important Information	Layout options apply only to the Detailed view. They are ignored when using the Icon view.
Included in Tasks	"Customize SiteScope Dashboard" on page 341

The Dashboard Layout dialog box includes the following elements:

GUI Element	Description
?	Click the **Show Descriptions** button to display additional information about the dialog box elements.
Dashboard Columns	You use the Dashboard Columns list to select optional columns to be displayed in the detailed tables. Your selections are applied to all applicable group and monitor elements. The columns available for display are: ➤ Description ➤ Monitor Type ➤ Monitored Target ➤ Summary Text ➤ Updated Timestamp ➤ Acknowledged ➤ Alerts Configured ➤ Alerts Triggered Select the Default columns option to display only the Name and Status columns. For details regarding the optional columns, see "SiteScope Dashboard - Current Status Tab" on page 363.
Dashboard refresh rate (sec)	Use this option to control the Dashboard refresh rate, in seconds. By default, the Dashboard view is automatically refreshed with the most recent monitor results every 30 seconds. You can set this value to be greater than 30 seconds. A value significantly less than 30 seconds may have a negative impact on SiteScope performance. The maximum value is 3600 seconds.
Maximum number of lines per initial table view	Enter the maximum number of lines for an initial view in a table. If a view exceeds this maximum, you can go to the next page.

GUI Element	Description
Objects per line	Use this option to restrict the display of monitor elements in Dashboard to a single line. The option affects monitors and groups status or description text requiring more than one text line for display. The default behavior is to display all summary text in multiple lines in the Dashboard view. When this option is enabled, the summary text is truncated to the amount of text that can be displayed on a single line for the applicable field. The full summary text is viewable as a tool tip when a user moves the pointer over the summary field.
Hide monitor availability	Select to hide icons in the Dashboard that indicate whether SiteScope was able to connect to a remote system or if a remote system was unavailable due to a connection problem. **Default**: Cleared. Dashboard includes availability icons.
Status Icon Tooltip	You can customize the tooltip by selecting the properties to display from the Status Icon Tooltip list. The properties available for display are: ➤ Description ➤ Monitor Type ➤ Monitored Target ➤ Summary Text ➤ Updated Timestamp ➤ Acknowledged ➤ Alerts Configured ➤ Alerts Triggered Select the Default option to display only the Name and Status in the tooltip.

Server Centric Report

Description	A graphical report showing the metrics CPU utilization, memory utilization, and network utilization for a selected server. **To access:** Click the server name link in the **Target** column of SiteScope Dashboard for a Windows Resource Monitor or UNIX Resource Monitor.
Important Information	This report is available only on those servers being monitored by a dedicated Windows Resource monitor or UNIX Resources monitor created for the purpose of running the report. It is highly recommended to deploy these monitors using the applicable solution templates for these monitors. The templates are preconfigured with the correct measurement counters and options already selected. **Note:** If a monitor encounters a problem and returns non-applicable data, that data point is skipped. Thus, you may see missing data points in the graph.
Included in Tasks	"Monitor Your Windows/UNIX Server's Resources" on page 346
Useful Links	"Generating a Server Centric Report" on page 337

The Server Centric Report includes the following elements:

GUI Element	Description
<Tooltip>	Hold the pointer over any data point on the graph to display a tooltip showing the value at the selected time of the utilization for the selected metric, as well as the date and time.
Server name	The name of the server appears above the Utilization graph.

GUI Element	Description
Time Range and Granularity bar	You can select the time range and granularity of the report using the Time Range and Granularity bar at the top of the report. For details, see "Choosing the Time Range and Granularity" in *Reference Information*. **Note:** To use the export functionality, you must add the SiteScope machine to the trusted sites.
Top 5 CPU Utilization Processes table	A table displaying the top five processes in terms of CPU utilization at any point in the graph. The table displays the process name and the CPU utilization value as a percent of total available CPU processing potential.
Top 5 Memory Consumption Processes table	A table displaying the top five processes in terms of memory consumption at any point in the graph. The table displays the process name and the memory consumption value in kilobytes.
Utilization graph	A graph displaying utilization over time. The different colored lines represent CPU utilization, memory utilization, and network utilization. All three metrics are scaled as percents (that is, out of 100% utilization). You can click on a data point in the graph to focus in on a shorter timer range. The data tables are updated to show results for the time of the data point you selected (clicking any of the three data points for the same time updates the report in the same way). This is useful when you notice a point with particularly high utilization. By clicking on the point, you can determine the cause of the high utilization. **Note**: Network utilization is supported for Windows servers only.

SiteScope Dashboard

Description	Displays current performance data for the infrastructure elements being monitored by SiteScope and provides access to features you use to define filters, layout options, and other view customizations. You can use the features in Dashboard to access individual monitor information by navigating or drilling down the group and monitor hierarchy. **To access:** Select an object in the Monitor Tree and click the **Dashboard** tab in the right pane.
Important Information	From the Dashboard, you can access the following SiteScope features: ➤ Server Centric Report ➤ Acknowledge Monitor Status ➤ Monitor Tools ➤ SiteScope Health Status ➤ Monitor History Information
Included in Tasks	"Analyze Data in SiteScope Dashboard" on page 343
Useful Links	"Overview of SiteScope Dashboard" on page 336

The Dashboard toolbar includes the following elements:

GUI Element	Description
☰	**Detailed view** displays groups and monitors in tabular list format with the element name, status, and other information arranged in individual table rows.
▦	**Icon view** displays groups and monitors as an array of status icons with the name of the element below the icon.
⊞	**Show child groups and monitors** displays only those elements that are direct children of the selected node. Subgroups and monitors are displayed in separate sections in the group and monitor status information area.

GUI Element	Description
⊞	**Show all descendent monitors** displays all descendent nodes of the selected node. In combination with the Detailed view option, monitors are displayed in areas divided by group context submenus that provide the path to the applicable groups. In combination with the Icon view option, only descendent monitor icons and names are displayed.
★+	Click the **Add Favorite** button to open the Add Dashboard Favorite dialog box which enables you to save the current Dashboard filter and layout settings as a favorite view.
★×	Click the **Delete Favorites** button to open the Delete Dashboard Favorites dialog box which enables you to delete existing favorite views.
▥	Click the **View or edit layout** button to open the Dashboard Layout page which enables you to customize the Dashboard display. For details, see “Dashboard Layout Page” on page 356.
▽	Click the **View or edit filter** button to open the Dashboard Filter page. For details, see “Dashboard Filter Page” on page 352.

GUI Element	Description
Favorite	The Favorite box contains a drop-down list of the existing favorite views of Dashboard filter and layout settings. You can select the one you want to display in the detailed view.
<Table Header path>	Enables you to see the position of the currently displayed view in the SiteScope hierarchy and to navigate to parent nodes using the path names displayed. The path can be expanded by clicking the icon on the left end of the path to show additional details about the current node or element, including acknowledgement data for the group. Clicking the down arrow on the Path opens an alert link menu for the context that enables you to add/delete acknowledgements, edit settings, enable/disable alerts or monitors, or to run monitors. Clicking the alert icon enables you to view the configured alerts for the group or container.

SiteScope Dashboard - Current Status Tab

Description	Displays a table of groups and monitors for the element highlighted in the monitor tree or listed in the path. You use features and links in the group and monitor status information area to navigate to child nodes and monitors and access other actions. **To access:** Click the Current Status tab within SiteScope Dashboard.
Included in Tasks	"Analyze Data in SiteScope Dashboard" on page 343

The Group and Monitor Status tables under the Current Status tab include the following elements (listed alphabetically):

GUI Element	Description
☰	Click the **Reset Column Width** button to restore the tables columns to their original width.
⏮ ◀ 1/1 Pages ▶ ⏭	Click to navigate through the results page by page or to jump to the first or last page.
☑	The **Acknowledge** column indicates that a SiteScope user has acknowledged the current status of a monitor and may have temporarily disabled alert actions associated with that monitor. This icon is only displayed in Dashboard Detailed views. Moving the pointer over the icon displays the acknowledgement information as a tool tip. For details, see "Acknowledging Monitor Status" on page 339.
⚠	The **Configured Alerts** column indicates that one or more alerts are associated with the group or monitor. If the pointer is passed over the icon, a tool tip displays the number of configured alerts. Clicking the icon displays the Configured Alerts window. Selecting an applicable alert definition name from the list changes the focus in the monitor tree to the subject alert definition and displays the alert properties view in the group and monitor status information area. For details, see "SiteScope Alerts" on page 1183.
⚡	The **Triggered Alerts** column indicates that at least one alert has been triggered in the monitor. If no alert was triggered, the icon is not displayed. If a single alert was triggered, an icon representing the specific alert type is displayed. If multiple alerts were triggered, an icon representing multiple alerts is displayed. Clicking the alert icon displays alert details. The Triggered Alert column only appears for a table that contains monitors. For details, see "SiteScope Alerts" on page 1183.

GUI Element	Description
Description	The **Description** column can contain either text that describes the monitor or group or it can contain HTML that performs various actions when you click it. You can enter information in the Description column by right-clicking either the monitor or the group in the monitor tree and then selecting **Edit**. In the page that opens in the group and monitor status information area, select **Advanced Settings** and scroll down to the **Description** text box.
Name	A display name (alias) for the monitor instance or group. When a new group is created, you enter its name. When a new monitor is created, you select its type from the list of available monitors. If you do not override this type in the **Name** field, the monitor is identified by the type of monitor. You can then optionally enter an alias that helps you identify this monitor. In a table for groups, you can click on the small black arrow in the Name column to open a context menu. For details, see "Name Column Context Menu" on page 368.
Status	A colored ball is displayed for each node in a Dashboard view, representing the operational status assigned to that component for its current performance level. You can point at the ball to display a tooltip which can be customized to show the information you choose. For details, see "Dashboard Layout Page" on page 356. A color-coded icon is also displayed for each element in a Dashboard view, representing the data availability status of the monitor. The monitor status and availability icons are described in "Status and Availability Levels" below.

GUI Element	Description
Summary	For monitors, the **Summary** column displays the most recent measurement results reported by the monitor. This may include more than one measurement, depending on the monitor type. For monitor groups, the summary displays the number of monitors within the group and the number of monitors, if any, that are reporting an error status.
Target	The **Target** column contains the name of the remote server containing the monitored object (if such a server exists). If, for example, the monitor type is CPU, then the target would be the name of the server on which the CPU being monitored is installed. The name displayed in the **Target** column can be either the system ID of the server or the user-assigned name (alias), depending on what was entered in the **Name** field when the server was added to the monitor tree. If the group contains a Windows Resource Monitor or UNIX Resource Monitor, the server name in the Target column appears as a link. You can click the link to open the Server Centric Report for the server. For details, see “Server Centric Report” on page 359.
Type	The type of monitor being displayed. You select the monitor type in the New Monitor page when you create the monitor instance.
Updated	The date and time when the last event occurred in the group or monitor.
Value	The value of the monitor counter when the monitor instance was last run. **Note:** This column appears only for a counter table displayed for a monitor.

Status and Availability Levels

Icon	Description
🟢	**OK Status**. All performance measurements are within the OK threshold level.
🟡	**Warning Status**. At least one performance measurement is within the Warning range, but no measurements are within the Error or Poor range.
🔴	**Error/Poor Status.** At least one performance measurement is within the Error or Poor range. This indicates either of the following: ➤ The performance measurement has a value, but at poor quality level. ➤ There is no measurement value due to some error.
⚪	**No thresholds breached Status.** No thresholds were defined for the monitor, so no status is assigned.
⇅	**Data Collected Availability.** Indicates that SiteScope was able to connect to the remote system and perform the action defined by the respective monitor configuration. The resulting monitor status represents the results of the monitor action. If an error or warning is indicated, it represents an accurate measure of the target system's performance or the availability of the target resource.
⇅	**Availability Warning.** Indicates that SiteScope has detected a possible problem with the connectivity to the remote system.
⇅	**No Data Availability.** Indicates that SiteScope was not able to connect to the remote system. Any resulting error status for the respective monitor may be attributed to the failure to communicate with a remote server. It does not necessarily mean the target resource has failed.

Name Column Context Menu

The following options are available by clicking the small black arrow in the Name column for Groups (listed alphabetically):

Menu Item	Description
Add Acknowledgement	Opens the Acknowledge dialog box which enables you to add an acknowledgement to a monitor.
Delete Acknowledgement	Deletes the monitor's acknowledgement.
Edit	Opens the Properties page for the selected group which enables you to edit the group's properties.
Enable/Disable Alerts in Group	Opens the Enable/Disable Alert Settings dialog box which enables you to enable or disable all the alerts for all monitors in the group. If you select **Disable**, the alerts are disabled until you return to this page and select **Enable**.
Enable/Disable Monitors in Group	Opens the Enable/Disable Monitor Settings dialog box which enables you to enable or disable all the monitors in the group. If you select **Disable**, the monitors are disabled until you return to this page and select **Enable**.
Run	Runs all the monitors in the group.

SiteScope Dashboard - Monitor History Tab

Description	Displays information about monitors, monitor groups, and alerts over the last 24 hours. This information is filtered by the number of hours, monitor status, and the number of data entries. **To access:** Click the Monitor History tab within SiteScope Dashboard.
Important Information	You enable this feature in General Preferences. You can determine exactly how much data you want saved for this feature so that your database does not get overloaded.
Included in Tasks	"Analyze Data in SiteScope Dashboard" on page 343
Useful Links	"Dashboard Monitor History View Options" on page 231

The Monitor History tab includes the following elements (listed alphabetically):

GUI Element	Description
⏮ ◀ 1/1 Pages ▶ ⏭	Click to navigate through the results page by page or to jump to the first or last page.
⚡	The **Triggered Alert** icon appears next to any monitor that triggered an alert.
Availability	This field only appears if you have selected **Show monitor availability** in the Details View pane of Dashboard Layout.
Group	The name of the group to which the monitor belongs. This field appears only if you have selected **Show all descendants** in Dashboard.
Name	The name of the monitor.
Run Time	The time the monitor ran.

GUI Element	Description
Status	The monitor's status at runtime (Error, Warning, or Good).
Summary	The description of the monitor run.

Part IV

Monitors

23

Working with SiteScope Groups

SiteScope groups are containers used to organize SiteScope monitor instances. This section provides an overview of concepts and details for working with SiteScope monitor groups.

About SiteScope Monitor Groups

SiteScope groups are tools for automatically connecting to and querying different kinds of systems and applications used in enterprise business systems.

Monitor instances that you create must be added within a SiteScope monitor group container. Monitor group containers may be nested within other group containers as subgroups. You use group containers to help you organize the monitor instances that you create.

Manage SiteScope Monitor Groups

The following sections describe the actions that you use with SiteScope groups. This includes a description of the steps you use to add, edit, delete, and perform other actions on groups.

Note: HTML code entered in monitor group text fields is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected.

Adding a Group to SiteScope

Groups can be added as a top level element within a SiteScope or as a subgroup within another monitor group container. You should create monitor group containers to make deployment of monitors and associated alerts manageable and effective for your environment and organization.

Groups can be added to SiteScope in more than one way. The simplest way it to add groups individually. Alternatively, you can deploy groups along with multiple monitors by using templates.

Use the following steps to add an group to SiteScope.

To add a monitor group using the left menu:

1. Using the left menu, select the SiteScope node or existing monitor group container into which you want add the group.
2. Right-click the container in the left menu to display the container action menu and select **New Group**. The New SiteScope Group page is displayed in the Contents panel.
3. Enter a name for the new group in the **Group Name** field.

4 Optionally, expand the Advanced Settings area and enter settings as applicable. See the section "SiteScope Group Settings" on page 617 for more details about Advanced Settings for groups.

5 When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the group.

To add a monitor to a group using the container Contents panel:

1 Using the left menu, select the SiteScope node or monitor group container into which you want add the group. The applicable container Contents panel is displayed.

2 Click the **New Group** button new the top of the Contents panel. The New SiteScope Group page is displayed in the Contents panel.

3 Enter a name for the new group in the **Group Name** field.

4 Optionally, expand the Advanced Settings area and enter settings as applicable. See the section "SiteScope Group Settings" on page 617 for more details about Advanced Settings for groups.

5 When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the group.

Editing a Group

Use the following steps to edit an existing group:

To edit a group using the left menu:

1 Using the left menu, select the monitor element that you want to edit.

2 Right-click the container in the left menu to display the container action menu and select **Edit**. The monitor properties edit page is displayed in the Contents panel.

3 Edit the monitor properties form as needed. See the help page for the applicable monitor type for information about the property settings.

4 When the required fields are complete, click the **OK** button at the bottom of the properties panel to update the monitor.

To edit a group using the container Contents panel:

1 Using the left menu, select the SiteScope or monitor group element to which you want to add a group. The applicable container Contents panel is displayed.

2 At the top of the Contents panel, click the **New Group** button. The monitor properties edit page is displayed in the Contents panel.

3 Edit the monitor properties form as needed. See the help page for the applicable monitor type for information about the property settings.

4 When the required fields are complete, click the **OK** button at the bottom of the properties panel to update the monitor.

Deleting a Group

Deleting a group removes the applicable monitor action from SiteScope and disables any alert action associated with the group. As with other actions, there is more than one method to delete a group.

To delete a group using the left menu:

1 Using the left menu, select the monitor element you want to delete.

2 Right-click the container in the left menu to display the container action menu and select **Delete**. A confirmation message is displayed.

3 Click **OK** to confirm the action. The monitor is deleted.

To delete a group using the container Contents panel:

1 Using the left menu, select the container or element to which the monitor is associated. The applicable Contents panel is displayed.

2 In the Monitors section of the Contents panel, check the box corresponding to the monitor (or monitors) you want to delete.

3 Click the **X** button at the bottom of the Monitors section to delete the selected monitor. A confirmation message is displayed.

4 Click **OK** to confirm the action. The monitor is deleted.

Copying a Group

You can copy an existing group and paste it to a new location within the SiteScope tree. Copying a group duplicates the configuration settings for the group and all monitors within the group.

After you copy a group, you normally need to edit the group and the configuration properties for each individual monitor within the group to direct the monitors to a unique system or application. Otherwise, the monitors in the group duplicate the monitoring actions of the original group.

Notes:

- Generally, you should avoid copying groups as it can lead to redundant monitoring. You can use templates to more efficiently replicate common group and monitor configuration patterns. See "Using SiteScope Templates" for more information about working with templates.
- To avoid group identity problems within SiteScope, object names must be unique within the parent container. If you copy a monitor group and paste it to a container in which there is another group with exactly the same name, SiteScope automatically adds a suffix (number) to the end of the monitor group's name.
- You cannot move or copy a monitor group to its subgroup.

Use the following steps to copy a group.

To copy a group using the left menu:

1. Using the left menu, select the monitor group you want to copy.
2. Right-click the container in the left menu to display the container action menu and select **Copy**.

3 Select the SiteScope node or monitor group node where you want the copy of the group to be created.

4 Right-click the container in the left menu to display the container action menu and select **Paste**. SiteScope adds a copy of the group to that selected node.

To edit a group using the container Contents panel:

1 Using the left menu, select the monitor group you want to copy. The applicable container Contents panel is displayed.

2 At the top of the Contents panel, click the **Copy icon** button.

3 Select the SiteScope node or monitor group node where you want the copy of the group to be created. The applicable container Contents panel is displayed.

4 At the top of the Contents panel of the target container, click the **Paste icon** button. SiteScope adds a copy of the group to that selected container node.

Moving a Group

You can move an existing group to a new location within the SiteScope tree. Moving a group duplicates the configuration settings for the group and all monitors within the group.

After you move a group, you normally need to edit the group and the configuration properties for each individual monitor within the group to direct the monitors to a unique system or application. Otherwise, the monitors in the group duplicate the monitoring actions of the original group.

Notes:

- Generally, you should avoid copying groups as it can lead to redundant monitoring. You can use templates to more efficiently replicate common group and monitor configuration patterns. See “Using SiteScope Templates” for more information about working with templates.
- To avoid group identity problems within SiteScope, object names must be unique within the parent container. If you move a monitor group and there is another group with exactly the same name in the same container, SiteScope automatically adds a suffix (number) to the end of the monitor group's name.

To move a group using the left menu:

1. Using the left menu, select the monitor group you want to copy.
2. Right-click the container in the left menu to display the container action menu and select **Cut**.
3. Select the SiteScope node or monitor group node where you want the copy of the group to be created.
4. Right-click the container in the left menu to display the container action menu and select **Paste**. SiteScope moves the group to that selected node.

To edit a group using the container Contents panel:

1. Using the left menu, select the monitor group you want to move. The applicable container Contents panel is displayed.
2. At the top of the Contents panel, click the **Cut icon** button.
3. Select the SiteScope node or monitor group node where you want to move the group. The applicable container Contents panel is displayed.
4. At the top of the Contents panel of the target container, click the **Paste icon** button. SiteScope moves the group to that selected container node.

Adding an Alert to a Group

You can create a group alert by adding an alert definition to a group container. By default a group alert is associated with all monitors within the group. This means that when any one monitor in the group reports the status category defined for the alert (for example, error or warning), the group alert is triggered. You can configure a group alert to exclude one or more of the monitors in the group by using the **Alert Targets** selection tree. Use the following steps to add an alert to a group.

To add an alert to a group using the left menu:

1 Using the left menu, select the monitor group container into which you want add the alert.

2 Right-click the container in the left menu to display the container action menu and select **New Alert**. The New Alert selection list is displayed in the Contents panel.

3 Click on the name of the alert type that you want to add. The alert properties page for the applicable monitor type is displayed.

4 Select the monitors that should trigger this alert. Complete the other alert properties as indicated. See the help page for the applicable alert type for information on system requirements and other detailed information about the property settings.

5 When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the alert definition.

To add an alert to a group using the container Contents panel:

1 Using the left menu, select the monitor group container into which you want add the alert. The applicable container Contents panel is displayed.

2 Click the **New Alert** button at the top of the Contents panel. The New Alert selection list is displayed in the Contents panel.

3 Click on the name of the alert type that you want to add. The alert properties page for the applicable monitor type is displayed.

4 Select the monitors that should trigger this alert. Complete the other alert properties as indicated. See the help page for the applicable alert type for information on system requirements and other detailed information about the property settings.

5 When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the alert definition.

Adding a Report to a Group

You can create a group report by adding a report definition to a group container. By default a group report includes data from all monitors within the group. You can configure a group report to exclude one or more of the monitors in the group by using the **Monitors and Groups to Report on** selection tree. Use the following steps to add an report to a group.

To add a report to a group using the left menu:

1 Using the left menu, select the monitor group container into which you want add the report.

2 Right-click the container in the left menu to display the container action menu and select **New Report**. The New SiteScope Report selection list is displayed in the Contents panel.

3 Click on the name of the report type that you want to add. The report properties page for the applicable monitor type is displayed.

4 Select the monitors whose data should be included in this report. Complete the other report properties as indicated. See the help page for the applicable report type for information about the property settings.

5 When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the report definition.

To add a report to a group using the container Contents panel:

1 Using the left menu, select the monitor group container into which you want add the report. The applicable container Contents panel is displayed.

2 Click the **New Report** button at the top of the Contents panel. The New SiteScope Report selection list is displayed in the Contents panel.

3 Click on the name of the report type that you want to add. The report properties page for the applicable monitor type is displayed.

4. Select the monitors whose data should be included in this report. Complete the other report properties as indicated. See the help page for the applicable report type for information about the property settings.
5. When the required fields are complete, click the **OK** button at the bottom of the properties panel to create the report definition.

24

Working with SiteScope Monitors

This chapter includes the main concepts and tasks for working with SiteScope monitors.

Overview of SiteScope Monitors

SiteScope monitors are tools for automatically connecting to and querying different kinds of systems and applications used in enterprise business systems. This section provides an overview of concepts and details for working with SiteScope monitors.

The different monitor types provide the generic capabilities for performing actions specific to different systems. You create one or more instances of a monitor type to instruct SiteScope how to monitor specific elements in your IT infrastructure.

For example, you can create 100 monitor instances that instruct the SiteScope CPU Monitor type to connect to and measure CPU utilization on remote servers. Each monitor instance contains a different setting defining which remote server is to be monitored and how often. SiteScope is then configured to automatically monitor the CPU utilization on 100 servers at regular intervals.

Monitor instances that you create must be added within a SiteScope monitor group container. Monitor group containers may be nested within other group containers as subgroups. You use group containers to help you organize the monitor instances that you create.

SiteScope Monitor Categories

SiteScope monitor categories are grouped according to classes that indicates their availability and category that reflect their function. When you select to add a new monitor to a SiteScope agent, the list of available monitor types for that agent are displayed both alphabetically and divided by category in the product interface. The availability of the monitor category is dependent on the class of monitor. This section describes the monitor classes and the category listing formats.

Solution Template Monitors

Solution template monitor types are a special class of monitors that enable new monitoring capabilities for specific applications and environments. As part of a solution template, these monitor types are deployed automatically together with other, standard monitor types to provide a monitoring solution that incorporates best practice configurations. These monitor types are controlled by option licensing and can only be added by deploying the applicable solution template. Once they have been deployed, you can edit or delete them using the same steps as with other monitor types. See the section "SiteScope Solution Templates Overview" for more information.

The monitor types using solution templates include:

- Active Directory (with and without Global Catalog)
- Exchange 5.5, 2000, 2003
- Oracle Database 8i, 9i, 10g
- SAP Application Server (NetWeaver and R3)
- Siebel App Server (for UNIX and for Windows)
- Siebel Gateway Server (for UNIX and for Windows)
- Siebel Web Server (for UNIX and for Windows)
- UNIX Resources Monitor
- WebLogic Application Server Monitor
- WebSphere Application Server Monitor
- Windows Resources Monitor

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. See the section for the particular monitor category for information on the usage and configuring each monitor type.

- **Application Monitors**. Monitors in this category monitor 3rd party applications. These monitors enable SiteScope to access and retrieve data from the monitored applications. For more information about Application Monitor capabilities, see the section on "Application Monitors" on page 407.
- **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. For more information about Database Monitor capabilities, see the section on "Database Monitors" on page 463.
- **Generic Monitors.** Monitors in this category monitor various type of environment. These monitors can monitor networks, applications, and databases depending on how they are configured. For more information about Generic Monitor capabilities, see the section on "Generic Monitors" on page 483.
- **Network Monitors.** Monitors in this category monitor network health and availability. For more information about Network Monitor capabilities, see the section on "Network Monitors" on page 501.
- **Server Monitors.** Monitors in this category monitor server health and availability. For more information about Server Monitor capabilities, see the section on "Server Monitors" on page 529.
- **Stream Monitors.** Monitors in this category monitor applications that play media files and stream data. For more information about Stream Monitor capabilities, see the section on "Stream Monitors" on page 549.
- **Web Transaction Monitors.** Monitors in this category monitor web-based applications. For more information about Web Transaction Monitor capabilities, see the section on "Web Transaction Monitors" on page 555.

Integration Monitors

This group of optional monitor types are used to integrate HP products with other commonly used Enterprise Management systems and applications. They are presented in a separate section on the New SiteScope Monitor panel.

These monitor types require additional licensing and may only be available as part of another HP product. For more information about Integration Monitor capabilities, see the section on "Working with SiteScope Integration Monitors" on page 899.

Monitoring Remote Servers

Some SiteScope monitors use Internet protocols to test Web systems and applications. Other SiteScope monitors use network file system services and commands to monitor information on remote servers. These monitors are limited to CPU, Disk Space, Memory, Service, Script (UNIX Only), NT Performance Counter, NT Event Log, and Web Server (Windows Only) monitors. This includes servers running the following operating systems:

- Windows XP/2000/2003
- Sun Solaris
- SGI Irix
- HP/UX
- Linux

Monitoring remote Windows servers requires SiteScope for Windows XP/2000/2003. In general, SiteScope for UNIX cannot monitor remote Widows servers.

The SiteScope service runs in a user or administrative account that has permission to access the Windows Performance registry on the remote servers to be monitored.

To change the user account of the SiteScope service:

1. Select **Start** > **Programs** > **Administrative Tools** > **Services** and click **SiteScope** from the list of services. The SiteScope Properties dialog box opens.
2. Click the **Log On** tab and fill in the **Log On As** fields with an account that can access the remote servers.
3. Click **OK** to save your settings and close the SiteScope Properties dialog box.
4. Right-click **SiteScope**. Click **Stop** to stop the SiteScope service.
5. Click **Start**. The SiteScope service now uses the new account.

To monitor certain server level parameters on a remote server using the network files system services, you need to create a remote server profile. A table of server profiles is listed on the Windows Servers or UNIX Servers pages. You access these pages from the Preferences menu. The remote server profiles contain the address and connection information that SiteScope needs to make a remote connection.

After creating remote server profiles, set up monitors to use the remote connection profile. For more information about remotely monitoring either Windows or UNIX servers, see “Windows Remote Preferences Overview” on page 195 or “UNIX Remote Preferences Overview” on page 201.

The requirements for monitoring services and applications that are running on remote servers vary according to the application and network policies in your environment. See the section “Overview of Ports Used for SiteScope Monitoring” below for more information about how SiteScope monitors connect to remote systems. You can also check the on-line Knowledge Base available from the Customer Support site for other information relating to monitoring remote servers.

Overview of Ports Used for SiteScope Monitoring

The following table lists the network ports that are generally used for SiteScope monitoring. In many cases, alternate ports may be configured depending on the security requirements of your environment.

Monitor Type	Ports Used
Apache Server Monitor	Port which Apache Server Admin pages located. Configurable via server configuration file.
ASP Server	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
BroadVision App Server	Uses the Object Request Broker (ORB) port number for the BroadVision server you are trying to monitor.
Checkpoint Firewall -1	SNMP monitor. Default is port 161.This is configurable.
Cisco Works	Cisco Works resources are usually available via port 161 or 162 (SNMP), depending on the configuration of the server.
Citrix Server	Ports 137, 138, and 139 (NetBIOS).
ColdFusion Server	Ports 137, 138, and 139 (NetBIOS).
CPU Utilization	For local CPU, no ports required. For CPUs on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS). For CPUs on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).
Database Query	This is configurable and depends on ODBC or JDBC driver and DB configuration.
DB2	Default is port 50000. This is configurable.
DHCP	Default is port 68.

Monitor Type	Ports Used
Directory	For local directory, no ports required. For directories on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS). For directories on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).
Disk Space	For local disk space, no ports required. For disk space on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS). For disk space on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).
DNS	Default is port 53.
Dynamo Application	Uses SNMP. This is configurable.
F5 Big IP	Uses SNMP. This is configurable.
File	Local disk. No ports required. For files on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS). For files on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).
FTP	Default is port 21.This is configurable.
IIS Server	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
iPlanet Server	Configurable via the iPlanet server administration page.
LDAP	The default is port 389. This is configurable.
Link Check	The default is port 80. This is configurable.
Log File	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.

Monitor Type	Ports Used
Mail	Port 110 for POP3, port 25 for SMTP, port 143 for IMAP.
MAPI	MAPI uses the Name Service Provider Interface (NSPI) on a dynamically assigned port higher than 1024 to perform client-directory lookup.
Memory	Ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Network	No ports required; monitors only the local machine.
News	Default is port 144. This is configurable.
NT Event Log	Ports 137, 138, and 139 (NetBIOS).
Windows Performance Counter	Ports 137, 138, and 139 (NetBIOS).
Oracle Database (JDBC)	This is configurable. Depends on target DB. Default is port 1521.
Oracle9i App Server	This is configurable. Port which Webcaching admin page located.
Ping	Default is port 7.
Port	Monitors any port.
Radius	Currently supports Password Authentication Procedure (PAP) authentication but not the Challenge Handshake Authentication Protocol (CHAP) or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). The RADIUS servers must be configured to accept PAP requests. Default is port 1645. In recent changes to the RADIUS spec, this may be changed to 1812. The monitor is configurable.
Real Media Player	Uses Real Media client on SiteScope box. Uses the port from which the media content is streamed (based on the URL).
Real Media Server	Ports 137, 138, and 139 (NetBIOS).

Monitor Type	Ports Used
RTSP	Uses the port from which the media content is streamed.
SAP	Uses SAP Client software (SAP Front End) to execute certain SAP transactions. Therefore, same ports as SAP.
Script	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Service	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
SilverStream	Configurable URL (Port number included in URL) to the applicable SilverStream server administration web page.
SNMP	Default is port 161. This is configurable.
SNMP Trap	Uses port 162 for receiving traps. This is configurable.
SQL Server	Ports 137, 138, and 139 (NetBIOS).
SunOne Webserver	URL to the stats-xml file on the target SunONE server. The port is configurable.
Sybase	Monitor requires Sybase Central client on the machine where SiteScope is running to connect to the Adaptive Server Enterprise Monitor Server. Port number the same as Sybase client.
Tuxedo	The default port for the TUXEDO workstation listener is port 65535. This is configurable.
URL	Generally port number 80. This is configurable.

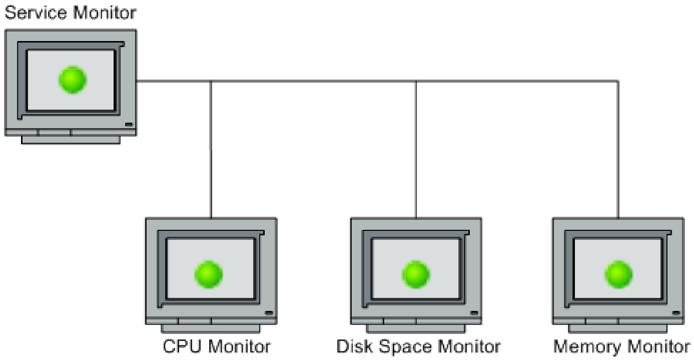
Monitor Type	Ports Used
Web Server	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Web Service	This is configurable.
WebLogic App Server	BEA WebLogic Application Server monitor uses the Java JMX interface. Port is configurable.
WebSphere App Server	Same port as the IBM WebSphere Administrator's Console.
WebSphere Performance Servlet	WebSphere Performance Servlet. Port is configurable.
Windows Media Player	Same port as media content to be monitored.
Windows Media Server	Ports 137, 138, and 139 (NetBIOS).

Monitoring Group Dependencies

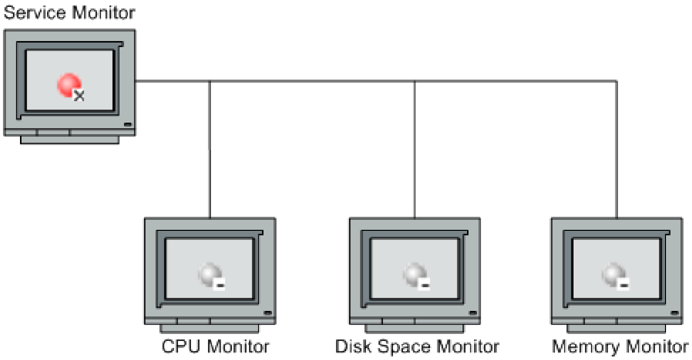
To prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system, select one monitor to check the basic availability of the system and then create other monitors that perform more detailed tests of that system. This creates a dependency relationship that enables you to make the running of a monitor group dependent on the status of a selected monitor.

Depends On

You use this option to make the running of this monitor dependent on the status of another monitor or monitor group. This can be used to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system. You can create a simple system monitor to check the basic availability or heartbeat of a system and then create other monitors that perform more detailed tests of that system. The figure below shows an example dependency relationship where three system monitors have been made dependent on a Service Monitor instance.



The detailed test monitors can be made dependent on the status of the heartbeat monitor by selecting that monitor. This means the dependent monitors run as long as the dependency condition is satisfied. If the heartbeat monitor detects that the target system has become unavailable, the dependency relationship automatically disables the other monitors. This has the effect of disabling any alerts that would have been generated by those monitors. The figure below shows the example monitors are disabled because the monitor upon which they depend is reporting an error condition.



By default, no dependency is set for a monitor instance. To make the running of the monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make a monitor dependent on the status of another monitor (by using the **Depends On** setting), you use this option to select the status category or condition that the **Depends On** monitor should have for the current monitor to run normally.

The status categories include:

- Good
- Error
- Available
- Unavailable

The monitor being configured is run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. If you have selected **Unavailable** and the **Depends On** monitor reports this status, the current monitors are not disabled.

For example, by selecting Good, this monitor is only enabled as long as the monitor selected in the **Depends On** field reports a status of Good. The current monitor is automatically disabled if the monitor selected in the **Depends On** field reports a category or condition other than the condition selected for this setting. See the examples for the Depends On setting.

Setting Status Thresholds

By setting performance boundaries, you can organize SiteScope performance data in a more meaningful way. You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system.

You can set status threshold criteria for each monitor instance to determine an error status, a warning status, and a good status. You can set up one or more status thresholds criteria for each status condition per monitor instance. Most monitor types include one default setting for each of the three status conditions. By default, only one threshold is displayed when you first configure the monitor.

When the monitor is not available, it is assigned a status that is based on the user definition in the **If Unavailable** drop-down list. A monitor can have a state of Unavailable as well as a status of Good/Warning/Error. Alerts are triggered according to availability, status, or both availability and status. For more details, see the Help page for the specific alert being defined.

While the monitor is enabled, it is assigned a status of good, warning, or error based on results returned by the most recent execution of the monitor action. The measurement taken or the results reported by the monitor are tested against all of the status threshold settings to determine the status that is reported for the monitor.

The individual threshold criteria results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status condition setting the status of the monitor is set to the highest valued status condition. For example, if one condition selected as Error if and another condition selected as Warning if are both met, the status would be reported as an error, with **error** being the highest value, **warning** the next highest and **good** the lowest value. The status is displayed by color and a status icon in the SiteScope interface.

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the monitor detects that the system has become unavailable, the status change from good to error is used to trigger an alert on error.

A change of status may also effect the state of a dependency between monitors. For example, a monitor that detects a change that results in a error status may be a trigger to disable one or more other monitors that are dependent on the system.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify.

For details on setting status thresholds, see "Set Thresholds for a Monitor" on page 403.

Setting Monitor Thresholds Using a Baseline

SiteScope includes options that allow you to monitor variations in response times and performance in the infrastructure. This allows a monitor to retain previous performance metrics to establish acceptable or expected performance ranges. When the monitor's performance exceeds that range by some value, the monitor can signal an error or warning. The activity involved in determining the expected performance characteristics is called baselining.

About Performance Baselines

Using the results or measurements collected from the monitors during the specified data collection period, a performance average (that is, baseline) and a standard deviation are calculated. The average establishes the baseline and when the performance of the monitor exceeds that baseline, either by a multiple of the standard deviation or a percentage difference from the baseline, the monitor may be considered in error.

The acceptable performance range of a monitor is determined by how far (variance) the current performance is from the baseline. This range of the variance may be based on multiples of the standard deviation or a multiples of a percentage difference.

For example, suppose a baseline for a monitor's round-trip time is 3 seconds and the standard deviation is 1.5 seconds. If the range for variance is selected as one times the standard deviation, then the monitor remains in a good condition as long as it’s round-trip time does not exceed 4.5 seconds. In another example, the baseline for a monitor's round-trip time is 5 seconds. The range for variance is selected as 50 percent of the baseline. The monitor remains in good status as long as it’s round-trip time does not exceed 7.5 seconds.

After the baseline has been set up for monitors, you can set baseline threshold criteria for each monitor. This is used to determine error, warning, and good threshold ranges for the monitor relative to the baseline data. The baseline value varies depending on the type of monitor.

Performance Baseline Types

SiteScope includes two baselining types: static and rolling. A static baseline is calculated once over an interval measured in days. A rolling baseline is calculated for an interval measured in monitor runs and the baseline value is updated after each monitor run.

Static Baseline

The static baseline feature calculates a one time, or fixed, baseline value based on monitor readings for a specified time period, staring from the current time. You specify the time interval in units of days. After sufficient data has been accumulated to calculate the baseline, SiteScope calculates a baseline value and displays this in the **Baseline status** field. It is this baseline value that is used as a comparison for subsequent monitor results. The baseline value displayed is a reference value of the baseline mean value, which varies depending on the type of monitor.

Rolling Baseline

To enable you to measure consistent response times and service levels for Web systems, SiteScope includes a rolling baseline. This helps to overcome the significant variations when measuring performance on the Internet over short periods of time. These variations may represent random changes in the number of client requests, in bandwidth usage from file downloads, or a systemic problem in the infrastructure. The rolling baseline is calculated for an interval measured in monitor runs. It is only available with the URL Monitor and Windows Performance Counter Monitor.

After sufficient data has been accumulated to calculate the baseline, SiteScope calculates a baseline value and displays this in the **Baseline status** field. The baseline value is recalculated and updated for each subsequent monitor run.

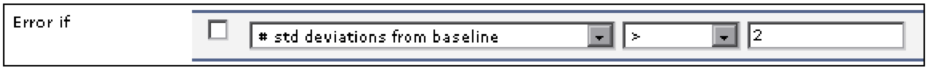
Setting Monitor Thresholds

After the baseline has been set up for monitors, each monitor must be edited to set the threshold range for the monitor relative to the baseline data. Each baselined monitor includes the following two thresholds in the Error if, Warning if, and Good if lists:

- # std dev from baseline
- % difference from baseline

Examples of Threshold Settings

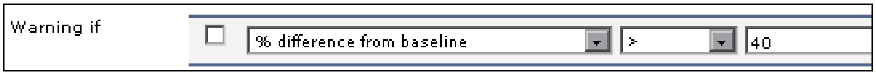
To set a monitor error threshold based on standard deviation from the baseline, select # std dev from the baseline option for the error, warning or good statuses. Then set a comparison operator such as > or >= and the number of standard deviations, such 2. As a result, the threshold would be set as in the following example:



Error if □ # std deviations from baseline > 2

This indicates that an error is any monitor value greater than two standard deviations from the baseline.

When using percent difference from baseline, you select a % difference from baseline option from the error, warning or good if drop-down list. Then set a comparator operator such as < or >= and then the number of standard deviations such a 40. As a result the threshold would be set as in the following example:



Warning if □ % difference from baseline > 40

This indicates that a warning status is any value greater than 40% of the baseline above the current baseline.

Monitor Properties for Static Baselines

As noted above, each baselined monitor includes the number of standard deviations from the baseline and the percent difference from the baseline as two available default threshold settings. Other performance properties are available for baselined monitors depending on the monitor type. The following table shows the SiteScope monitor type and the corresponding measurements available for that type:

Monitor Type	Properties
Apache	CPU load
ASP	errors per second
Asset **Note:** This monitor appears only if there is an assets directory below the installed SiteScope directory.	round-trip time
Check Point	rejected
ColdFusion	page hits per second
CPU	% cpu used
Database Query	round-trip time
Directory	total file sizes
Disk	% full
DNS	round-trip time
File	file age
FTP	round-trip time
IIS	bytes sent per second
IPlanet	bytes transferred
LDAP	round-trip time
Link Check	number of link errors
Log File	matches per minute

Monitor Type	Properties
Mail	round-trip time
Memory	% full
Network	bytes sent per second
News	round-trip time
Ping	round-trip time
Port	round-trip time
Radius	round-trip time
RTSP	bytes downloaded
Script	round-trip time
Service	status
SilverStream	hits per second
SNMP	OID value
URL	round-trip time
URL Sequence	round-trip time
Web Service	hits per minute
Windows Performance Counter	first counter
Windows Dialup	total time
Windows Event Log	match count

For details on enabling a baseline and setting thresholds, see “Set Monitor Thresholds Using a Static Baseline” on page 404 and “Set Monitor Thresholds Using a Static Baseline” on page 404.

Deploy a Monitor

To deploy a monitor, you must first create a monitor group container, and then add monitors to the monitor group container. You can also copy an existing monitor and paste it into any monitor group in the SiteScope tree.

Create a Monitor Group

You create monitor instances within a SiteScope monitor group container. For details, see "Manage SiteScope Monitor Groups" on page 374.

Create a Monitor

Select the monitor group container into which you want to add the monitor. Click the monitor name for the monitor type you want to add, and complete the monitor properties form. For details, see "Configuring New SiteScope Monitor" on page 615.

Copying a Monitor

You can copy an existing monitor and paste the copy into any monitor group in the SiteScope tree. Copying a monitor duplicates the configuration settings for the monitor.

After you copy a monitor, you normally need to edit the monitor to change the system or application that the monitor is targeting. Otherwise, the copied monitors duplicate the monitoring actions of the original monitor.

For details, see "Monitor Context Menu Options" on page 163.

Set Thresholds for a Monitor

You set logic conditions that determine the reported status of each monitor instance using the Threshold Settings section. For details, see "Threshold Settings" on page 608.

Optionally, you can set thresholds using a static or rolling baseline. For details, see "Set Monitor Thresholds Using a Static Baseline" on page 404 and "Set Monitor Thresholds Using a Rolling Baseline" on page 405.

Set Monitor Thresholds Using a Static Baseline

You can set monitor thresholds using a static baseline by enabling the baseline and setting threshold ranges.

Enable a Static Baseline

To enable a static baseline for a monitor, right-click the monitor and select **Edit**. In the **Threshold Settings** area, click the **Baseline** button, and enter the baseline data interval you want to use for this monitor for gathering statistics. For details, see "Threshold Settings" on page 608.

To enable static baselines for multiple monitors, use the Global Replace Wizard. In the Choose Changes page, expand **Threshold Settings**, select the **Activate baselining** and **Number of days used for baselining calculation** check boxes, and enter the baseline data interval. For details, see "Global Search and Replace Wizard" on page 279.

Important: After you have selected and enabled monitors for baselining, you should allow the monitors to run for a period at least as long as the baseline period you want to use to allow the monitors to accumulate data for the baseline period.

Set Monitor Threshold Ranges

After accumulating monitoring data for the baseline interval period, SiteScope calculates a baseline value and displays this in the **Baseline status** field of the **Threshold Settings**.

Edit the configuration settings for the baselined monitors to make use of the baseline data. In the **Threshold Settings** area, set the monitor threshold ranges (error, warning, and good) to be calculated relative to the baseline data. For details, see "Threshold Settings" on page 608.

Note: The calculated baseline value varies depending on the type of monitor. For a list of SiteScope monitor types and the corresponding measurements, see “Setting Monitor Thresholds” on page 400.

Set Monitor Thresholds Using a Rolling Baseline

You can set monitor thresholds using a rolling baseline by activating the baseline calculation and setting threshold ranges. Rolling baseline is only applicable to the URL Monitor and Windows Performance Counter Monitor.

Enable a Rolling Baseline

To enable a rolling baseline for a monitor, right-click a monitor and select **Edit**. In the **Advanced Settings** area, enter the number of monitor runs to be used to calculate the baseline in the **Baseline Interval** box. For details, see “Windows Performance Counter Monitor Settings” on page 828 or “URL Monitor Settings” on page 858.

To enable rolling baselines for multiple monitors, use the Global Replace Wizard. In the Choose Changes page, expand **Advanced Settings**, select the **Baseline Interval** check box, and enter the number of monitor runs to calculate the baseline. For details, see “Global Search and Replace Wizard” on page 279.

Important: After you have selected and enabled monitors for baselining, you should allow the monitors to run for a period at least as long as the baseline period you want to use to allow the monitors to accumulate data for the baseline period.

Set Monitor Threshold Ranges

After accumulating monitoring data for the baseline interval period, SiteScope calculates a baseline value and displays this in the **Baseline status** field of the **Threshold Settings**. The baseline value is recalculated and updated for each subsequent monitor run.

Edit the configuration settings for the baselined monitors to make use of the baseline data. In the **Threshold Settings** area, set the monitor threshold ranges (error, warning, and good) to be calculated relative to the baseline data. For details, see "Threshold Settings" on page 608.

Disable Rolling Baseline Calculation

To disable a rolling baseline calculation for a monitor, right-click the monitor and select **Edit**. In the **Advanced Settings** area, clear the value in the **Baseline Interval** box. In the **Threshold Settings** area, set the error, warning, and good threshold ranges to something other than baseline related data (that is to say, a setting that does not contain deviation percentage, # std dev from baseline or % difference from baseline). For details, see "Advanced Settings" on page 603 and "Threshold Settings" on page 608.

25

Application Monitors

This chapter includes information about monitoring third-party applications. The monitors described enable SiteScope to access and retrieve data from the monitored applications.

Active Directory Replication Monitor Overview

Use the Active Directory Replication Monitor to monitor the time that it takes a change made on one Domain Controller to replicate to up to as many as ten other Domain Controller. This allows 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.

Note:

- The Active Directory Replication Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- This monitor can only be added by deploying an Active Directory Solution template. For information on using templates to deploy monitors, see "Using SiteScope Templates" on page 1039.

No additional setup is required other than to allow 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 computed.

For details on configuring this monitor, see "Active Directory Replication Monitor Settings" on page 621.

ASP Server Monitor Overview

Use the ASP Server Monitor to monitor the server performance parameters for Microsoft ASP servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each ASP Server you are running.

The Remote Registry service must be running on the machine where the ASP server is running if the ASP Server is running on Windows 2000.

The ASP Server Monitor makes use of Performance Counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you need to define the connection to these servers under the Windows Remote Preferences option in the SiteScope Preferences.

For details on configuring this monitor, see "ASP Server Monitor Settings" on page 623.

Apache Server Monitor Overview

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 allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Apache server you are running.

Setup Requirements for the Apache Server Monitor

Before you can use the Apache Server Monitor, you need to 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.
- The SiteScope Apache Server Monitor currently supports the server status page available at http://<server_address>:<port>/server-status?auto. The port is normally port 80, although this may vary depending on the server set up and your environment. For some Apache server configurations you may need to use the server name rather than an IP address to access the server statistics page.

Configuring This Monitor

For details on configuring this monitor, see “Apache Server Monitor Settings” on page 625.

BroadVision Application Server Monitor Overview

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 allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each BroadVision server in your environment.

You need to 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.

For details on configuring this monitor, see "BroadVision Application Server Monitor Settings" on page 627.

Check Point Firewall-1 Monitor Overview

Use the Check Point Firewall-1 Monitor to monitor the content of event logs and other data from Check Point Firewall-1 servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate Check Point Firewall-1 monitor instance for each Check Point Firewall-1 server in your environment.

For details on configuring this monitor, see "Check Point Firewall-1 Monitor Settings" on page 628.

Cisco Works Monitor Overview

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 allows you to watch server loading for performance, availability, and capacity planning. Create a separate Cisco Works monitor instance for each Cisco Works server in your environment.

For details on configuring this monitor, see "Cisco Works Monitor Settings" on page 630.

Citrix Server Monitor Overview

The Citrix Server Monitor makes use of Performance Counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you need to define the connection to these servers under the NT Remotes option in the SiteScope Preferences.

The Citrix Server Monitor allows you to monitor the server performance statistics from Citrix Metaframe Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate Citrix monitor instance for each Citrix Server in your environment.

Setup Requirements for the Citrix Server Monitor

The following are important requirements for using the SiteScope Citrix Server Monitor:

- The Remote Registry service must be running on the machine where the Citrix Server is running if Citrix is running on a Windows 2000 platform.
- The Citrix Resource Manager must be available, installed, and running on the Citrix servers you want to monitor.

- One or more Citrix vusers need to have established a connection with the Citrix server to enable viewing of ICA Session object.
- The Citrix Server Monitor requires the same permissions (trust level between monitoring and monitored machines) in Windows 2003 as Windows Resources monitor. For details, see "Configuring the Windows Resources Monitor to Run on Windows 2003 as a Non-Administrator User" on page 545.

Troubleshooting Tips for the Citrix Server Monitor

The following are troubleshooting tips for the Citrix Server Monitor:

1. Open a command line window (DOS prompt)
2. Type the following command, substituting the host name as appropriate:

```
C:\>perfex \\hostname -u username -p password -h | find "ICA"
```

3. This should return a response like the following:

```
(3378) ICA Session
(3386) ICA Session
(3379) This object has several counters that can be used to monitor the
performance in ICA sessions
(3387) This object has several counters that can be used to monitor the
performance in ICA sessions"
ICA Session" 3386    performance in ICA sessions
```

If you do not see something like the above response, then either the counters are not available on the remote server or you get a more descriptive error message indicating what might be the problem.

Configuring This Monitor

For details on configuring this monitor, see "Citrix Server Monitor Settings" on page 633.

ColdFusion Server Monitor Overview

The ColdFusion Server Monitor makes use of Performance Counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you need to define the connection to these servers under the Windows Remote Preferences option in the SiteScope Preferences container.

Use the ColdFusion Monitor to monitor the server performance statistics from ColdFusion servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate ColdFusion monitor instance for each ColdFusion server in your environment.

The Remote Registry service must be running on the machine where the ColdFusion server is running if ColdFusion is running on Windows 2000.

For details on configuring this monitor, see “ColdFusion Server Monitor Settings” on page 634.

COM+ Server Monitor Overview

You use the COM+ Server Monitor to monitor the performance of software components registered and running on Microsoft COM+ servers. When you specify the host and port number of this probe instance, SiteScope retrieves all the functions running on the COM+ server for your monitoring selection. Error and warning thresholds for the monitor can be set on one or more function measurements.

Note: The COM+ Server Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

Setup Requirements for the COM+ Server Monitor

The following are several key requirements for using the COM+ Server Monitor:

- A COM+ probe component from HP must be installed and running on the target COM+ server you want to monitor.
- There must be HTTP connectivity between the SiteScope server and the server running the COM+ probe.
- To enable this monitor type in SiteScope, an Option license for the COM+ Monitor must be obtained and input into SiteScope.

Note: You cannot have multiple SiteScope instances share one probe instance. You can have multiple COM+ 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.

COM+ Probe Installation

The COM+ probe is available from the HP Customer Support download site. You must log in with your HP user name and password to access the Customer Support Downloads page.

After downloading, follow the instructions for installing the probe on the COM+ server to be monitored.

Once the probe is successfully installed, you must start it prior to running or defining a SiteScope COM+ 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\.

COM+ Functions

After you have specified the COM+ Probe for the target COM+ Server, you use the Browse Counters Utility in the monitor configuration page. The COM+ probe is queried for a list of available functions to monitor, and a browse tree is displayed. See the Browsable Counter Utility help page for instructions on how to navigate this hierarchy tree and select your functions or counters of interest.

Configuring This Monitor

For details on configuring this monitor, see “COM+ Server Monitor Settings” on page 636.

Dynamo Application Server Monitor Overview

Use the Dynamo Application Server Monitor to monitor the server performance data for ATG Dynamo servers using SNMP. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each ATG Dynamo server in your environment.

For details on configuring this monitor, see “Dynamo Application Server Monitor Settings” on page 638.

F5 Big-IP Monitor Overview

Use the F5 Big-IP Monitor to monitor the content of event logs and other data from F5 Big-IP load balancing device. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate F5 Big-IP monitor instance for each F5 Big-IP load balancing device in your environment.

For details on configuring this monitor, see "F5 Big-IP Monitor Settings" on page 640.

IIS Server Monitor Overview

Use the Microsoft IIS Server Monitor to monitor the server performance statistics from IIS servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate IIS Server monitor instance for each IIS server in your environment.

The IIS Server Monitor makes use of Performance Counters to measure application server performance. SiteScope must be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you need to define the connection to these servers under the Windows Remote Preferences option in the SiteScope Preferences container.

The Remote Registry service must be running on the machine where the IIS server is running if IIS is running on Windows 2000.

For details on configuring this monitor, see "IIS Server Monitor Settings" on page 643.

iPlanet Server Monitor Overview

The SiteScope iPlanet Server Monitor is formerly known as the Netscape Server Monitor. Several file, name, and performance counter changes have been made to reflect the changes in the server product name and capabilities of the monitor.

Use the iPlanet Server Monitor to monitor the content of server administration pages for iPlanet and Netscape servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each server you are running.

Setup Requirements for the iPlanet Server Monitor

The following are requirements for using the iPlanet Server Monitor:

To monitor current activity statistics for iPlanet 4.1 servers:

1. You need to know the user name and password to access the iPlanet administrative server page. The URL for the main administrative page normally has the format http://serveraddress:adminport/https-admserv/bin/index
2. Identify the virtual server instance name you want to monitor. This should be available in the drop-down box to the right of the **Manage** button. Enter it in the place of **virtualserveraddressname** in the URL (see below).
3. Set up monitor using iPlanet 4.1 current activity counters using the URL of the following format http://serveraddress:adminport/https-virtualserveraddressname/bin /sitemon?doit:

To monitor performance dump statistics for iPlanet 4.1 servers:

1. Modify the **obj.conf** file for each virtual server instance you want to monitor adding the line to enable perf dump. The **conf** entry normally has the format
<Object path="path/Netscape/Server4/docs/.perf">Service fn=service-dump
</Object>.
2. Restart the servers.
3. Access the performance dump page using the URL with the format
http://serveraddress:http_port/.perf.
4. Set up the iPlanet Server Monitor using iPlanet 4.1 performance dump counters (see below).

To monitor server statistics for iPlanet 6.0 servers using HTTP:

1. You need to know the user name and password to access the iPlanet administrative server page. The URL for the main administrative page normally has the format
http://serveraddress:adminport/https-admserv/bin/index
2. Identify the specific server instance names as shown in the drop-down box next to the **Manage** button. The server instance names are used as the virtualserveraddressname the URL for monitoring that server instance.

   The URL needed to monitor the server statistics normally has the format:

   http://serveraddress:adminport/https-virtualserveraddressname/
bin/instance-app/<pageStats>.jsp?pollInterval=15&vsname=All

   where <pageStats> is replaced with a specific statistics page name as outlined below.

Note:

For the value for vsname (virtual server name), you can replace all with a specific virtualserveraddressname to monitor specific server instances. For example,
http://serveraddress:adminport/https-virtualserveraddressname/bin
/instance-app/ pageStats.jsp?pollInterval=15&vsname=
virtualserveraddressname

- To monitor virtual server activity statistics, substitute <virtualServerStats> for <pageStats>.
- To monitor server connection status statistics, substitute <connectionStats> for <pageStats>.
- To monitor server DNS statistics for iPlanet 6.0 servers, substitute <dnsStats> for <pageStats>.
- To monitor Keep-Alive statistics, substitute <keepAliveStats> for <pageStats>.

Scheduling This Monitor

Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Update value of several minutes to allow the server to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.

Configuring This Monitor

For details on configuring this monitor, see “iPlanet Server Monitor Settings” on page 645.

News Monitor Overview

Running the News Monitor on a regular basis can save you the headaches associated with the entire office coming in to tell you they can not read their news groups. With regular monitoring, you should be able to address problems before they impact the users.

In addition, you can manage the number of articles that are allowed to queue up, deleting them before they cause disk space problems.

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 allow 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 Advanced Settings section of the monitor.
- login failed, unauthorized - the user name and password were not accepted by the news server

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

Configuring This Monitor

For details on configuring this monitor, see “News Monitor Settings” on page 648.

Oracle9i Application Server Monitor Overview

Use the Oracle9i Application Server Monitor to monitor the server performance data for Oracle9i servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Oracle9i Application server in your environment.

Note: You must enable Web caching on the Oracle 9i Application Server to use the Oracle9i Application Server Monitor.

For details on configuring this monitor, see “Oracle 9i Application Server Monitor Settings” on page 649.

Oracle10g Application Server Monitor Overview

Use the Oracle10g Application Server Monitor to monitor the server performance data for Oracle10g servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Oracle10g Application server in your environment.

Note: By default, the Oracle 10g metrics servlet is visible only to the local host. To enable monitoring the Oracle 10g application server, the servlet must be accessible from other IP addresses. You must edit the **dms.conf** file in the **<Oracle 10g installation path>infra/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 be able to see the following URL: **http://<Oracle 10g machine URL>:7201/dmsoc4j/Spy?format=xml**.

For details on configuring this monitor, see “Oracle10g Application Server Monitor Settings” on page 652.

Radius Monitor Overview

The Radius Monitor is useful for testing that the RADIUS server is correctly handling authentication requests. If the RADIUS server fails, any users that try to use it are unable to login and access any services. Setup a Radius monitor for each RADIUS server in your environment. You may want to setup multiple monitors per server if you want to test different kinds of login accounts.

In order for SiteScope to monitor your RADIUS server you must first add the IP address of your SiteScope server to the list of Clients that the RADIUS server is allowed to communicate with. This must be done in order for the Radius Server to take requests from SiteScope. Failure to do this results in Unknown Client errors on the RADIUS server.

The Radius Monitor currently supports Password Authentication Procedure (PAP) authentication but not the Challenge Handshake Authentication Protocol (CHAP) or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). Your RADIUS server must be configured to accept PAP requests to use this monitor.

Status

Each time the Radius Monitor runs, it returns a status message and writes it in the monitoring log file. It also writes the total time it takes to receive a authentication response.

The reading is the current value of the monitor. The possible values for the Radius Monitor are:

- OK
- unknown host name
- timed out reading
- match error

The status is logged as either good or error. An error status is returned if the current value of the monitor is anything other than OK.

Configuring This Monitor

For details on configuring this monitor, see “Radius Monitor Settings” on page 654.

SAP CCMS Monitor Overview

The SAP CCMS Monitor retrieves and reports metrics using SAP's new centralized monitoring architecture, CCMS (Computer Center Management System). With CCMS, a SAP administrator can monitor all servers, components and resources in the R/3 landscape from a single centralized server, greatly facilitating not only problem discovery but also problem diagnosis.

Note: The SAP CCMS Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

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 via the CCMS interface.

Note: Due to the large amount of metrics that are being retrieved when displaying the entire SAP metrics browse tree during monitor definition, there could be a noticeable delay going from the Choose Server page to the Choose Counters page (possibly 1 to 2 minutes). However, once 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.

This monitor only retrieves and displays numeric metrics (Performance attributes). That is, Status, Log and Information attributes are currently not supported. Also, presentation and management of SAP CCMS Alerts in SiteScope are not supported at this time.

Software Requirements

- The SAP CCMS Monitor requires that the SAP Java Connector (SAP JCo 2.0.6 and above) component be downloaded from the SAP Service Marketplace Software Distribution Center, and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location). For details, see “SAP Java Connector Installation” on page 431.
- The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and above only.
- Consult your SAP documentation to determine if your R/3 landscape components may need additional software installed to run or work with CCMS.

To download SAP Java Connector, go to the SAP Software Distribution Center at:

http://www.service.sap.com/connectors

Click **SAP Java Connector** and then click **Tools and Services**.

Note: You need a valid Service Marketplace login to access this SAP Web site.

User Authorization

A SAP user requires certain privileges to read CCMS metrics. When defining a SAP CCMS Monitor in SiteScope you must specify a user who has XMI authorization to be able to login to the CCMS server and retrieve metrics. The user should have one or more of the profiles listed below assigned to it. Authorizations are collected in SAP profiles, and the following profiles include XMI authorization:

- S_A.SYSTEM
- PD_CHICAGO
- S_WF_RWTEST
- SAP_ALL

One test to see if a user has such authorization is to try and issue transaction RZ20 in the SAP GUI and see if the CCMS monitor sets can be displayed.

SAP Java Connector Installation

The SAP CCMS monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the appropriate license granted by SAP to receive and use these libraries.

To enable the SAP CCMS monitor on a Windows environment:

1. Download the following .jar file and .dll files from the SAP support Web site:
   - **sapjco.jar**
   - **librfc32.dll**
   - **sapjcorfc.dll**
2. Copy the **sapjco.jar** file into the <**SiteScope root directory**>**/WEB-INF/lib** directory.
3. Copy the two .dll files into the <**SiteScope root directory**>**/bin** directory.

Note: Check if the .dll files already exist in the <**Windows installation directory**>**/system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

4. Restart SiteScope.

To enable the SAP CCMS monitor on a UNIX environment:

1. Download the following .jar file and .so files from the SAP support Web site:
   - **sapjco.jar**
   - **librfccm.so**
   - **libsapjcorfc.so**
2. Copy the **sapjco.jar** file into the <**SiteScope root directory**>**/WEB-INF/lib** directory.

3 Copy the two .so files as follows:

- For Sun installations, copy into the <**SiteScope root directory**>**/java/bin/sparc** directory.
- For Linux installation, copy into the <**SiteScope root directory**>**/java/bin/i386** directory.

4 Restart SiteScope.

Scheduling This Monitor

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Frequency** setting. Note, however, that CCMS metrics are generally only updated once every 5 minutes.

Configuring This Monitor

For details on configuring this monitor, see “SAP CCMS Monitor Settings” on page 656.

SAP CCMS Alerts Monitor Overview

The SAP CCMS Alerts Monitor retrieves and reports alerts from the SAP CCMS monitors using SAP's centralized monitoring architecture: CCMS (Computer Center Management System). Using SAP's advanced CCMS interface BC-XAL 1.0, this new SiteScope monitor retrieves alerts.

The SAP CCMS Alerts Monitor allows you to monitor and complete alerts for various components of your R/3 landscape.

Note: The SAP CCMS Alerts Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

Software Requirements

To enable the SAP CCMS Alerts monitor, you must install the SAP Java Connector. For details, see "SAP Java Connector Installation" on page 431.

The SAP Java Connector (SAP JCo 2.0.6 and above) component must be downloaded from the SAP Service Marketplace Software Distribution Center and installed on the same server where SiteScope is running (or at least be accessible on a shared or remote location).

To download SAP Java Connector, go to http://www.service.sap.com/connectors.

Click **SAP Java Connector**, **Tools and Services**. You need a valid Service Marketplace login to access this site.

Note: The BC-XAL 1.0 interface is supported on R/3 systems 4.5B and above only.

Consult your SAP documentation to determine if your R/3 landscape components need additional software installed to run or work with CCMS.

User Authorization

A SAP user requires certain privileges to read CCMS metrics. When defining a SAP CCMS Alerts Monitor in SiteScope you must specify a user who has XMI authorization to be able to login to the CCMS server and retrieve metrics. The user should have one or more of the profiles listed below assigned to it. Authorizations are collected in SAP profiles, and the following profiles include XMI authorization:

- S_A.SYSTEM
- PD_CHICAGO
- S_WF_RWTEST
- SAP_ALL

One test to see if a user has such authorization is to try and issue transaction RZ20 in the SAP GUI and see if the CCMS monitor sets can be displayed.

SAP Java Connector Installation

The SAP CCMS Alerts monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the appropriate license granted by SAP to receive and use these libraries.

To enable the SAP CCMS Alerts monitor on a Windows environment:

1 Download the following .jar file and .dll files from the SAP support Web site:

- **sapjco.jar**
- **librfc32.dll**
- **sapjcorfc.dll**

2 Copy the **sapjco.jar** file into the <**SiteScope root directory**>**/WEB-INF/lib** directory.

3 Copy the two .dll files into the <**SiteScope root directory**>**/bin** directory.

Note: Check if the .dll files already exist in your <**Windows installation directory**>**/system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

---

4 Restart SiteScope.

To enable the SAP CCMS Alerts monitor on a UNIX environment:

1 Download the following .jar file and .so files from the SAP support Web site:

- **sapjco.jar**
- **librfccm.so**
- **libsapjcorfc.so**

2 Copy the **sapjco.jar** file into the <**SiteScope root directory**>**/WEB-INF/lib** directory.

3 Copy the two .so files as follows:

- For Sun installations, copy into the <**SiteScope root directory**>**/java/bin/sparc** directory.
- For Linux installation, copy into the <**SiteScope root directory**>**/java/bin/i386** directory.

4 Restart SiteScope.

Scheduling This Monitor

The default run schedule for this monitor is every 10 minutes, but you can change it to run more or less often using the **Update every** setting. Note, however, that CCMS metrics are generally only updated once every 5 minutes.

Configuring This Monitor

For details on configuring this monitor, see “SAP CCMS Alerts Monitor Settings” on page 658.

SAP Java Web Application Server Monitor Overview

The SiteScope SAP Java Web Application Server monitor allows you 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 presents a counter tree for each dispatcher and server in the cluster.

Note: The SAP Java Web Application Alerts Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

To enable the SAP Java Web Application Server monitor, you must install the SAP JMX Connector. For details, see below.

SAP JMX Connector Installation

The SAP Java Web Application Server monitor uses SAP JMX Connector libraries to connect to SAP J2EE cluster. A user must have the appropriate license granted by SAP to receive and use these libraries.

To enable the SAP Java Web Application Server monitor:

1 Rename the **logging.jar** file from the SAP Java Web Application server to **sap_logging.jar** so as not to overwrite the SiteScope **logging.jar** file.

2 Copy the following .jar files from the SAP Java Web Application server installation:

➤ **admin.jar**

➤ **com_sap_pj_jmx.jar**

➤ **exception.jar**

➤ **sap_logging.jar** (renamed from **logging.jar** in SAP library)

➤ **jmx.jar**

into the <**SiteScope root directory**>**/WEB-INF/lib** directory.

3 Restart SiteScope.

Configuring This Monitor

For details on configuring this monitor, see "SAP Java Web Application Server Monitor Settings" on page 660.

SAP Work Processes Monitor Overview

The SAP Work Processes Monitor allows you to monitor the effectiveness of your SAP R/3 server configurations. The monitor provides statistical information on work process performance. This information allows you to estimate whether the SAP R/3 Server is efficiently using its resources.

Note: The SAP Work Processes Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

To enable the SAP Work Processes monitor, you must install the SAP Java Connector. For details, see below.

Understanding the SAP Work Processes Monitor

A SAP work process is a program that executes 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.

SAP Java Connector Installation

The SAP Work Processes monitor uses SAP JCo libraries to connect to the SAP R/3 system. A user must have the appropriate license granted by SAP to receive and use these libraries.

To enable the SAP Work Processes monitor on a Windows environment:

1 Download the following .jar file and .dll files from the SAP support Web site:

- **sapjco.jar**
- **librfc32.dll**
- **sapjcorfc.dll**

2 Copy the **sapjco.jar** file into the **<SiteScope root directory>/WEB-INF/lib** directory.

3 Copy the two .dll files into the **<SiteScope root directory>/bin** directory.

Note: Check if the .dll files already exist in the **<Windows installation directory>/system32** directory. They may have been copied into this directory as part of the SAP client installation. If they do exist in your system, you must overwrite them with the above .dll files before copying into the SiteScope directory.

4 Restart SiteScope.

To enable the SAP Work Processes monitor on a UNIX environment:

1. Download the following .jar file and .so files from the SAP support Web site:
   - **sapjco.jar**
   - **librfccm.so**
   - **libsapjcorfc.so**
2. Copy the **sapjco.jar** file into the <**SiteScope root directory**>**/WEB-INF/lib** directory.
3. Copy the two .so files as follows:
   - For Sun installations, copy into the <**SiteScope root directory**>**/java/bin/sparc** directory.
   - For Linux installation, copy into the <**SiteScope root directory**>**/java/bin/i386** directory.
4. Restart SiteScope.

Configuring This Monitor

For details on configuring this monitor, see "SAP Work Processes Monitor Settings" on page 662.

Siebel Application Server Monitor Overview

The Siebel Application Server Monitor (previously know as the Siebel Server Manager Monitor) uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel application servers.

Note: The Siebel Application Server Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

System Requirements

The following are requirements for using the Siebel Application Server Monitor:

1. The Siebel Server Manager client must be installed on the machine where SiteScope is running or accessible to the SiteScope machine. 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.
   - For Windows networks, map the network drive where the Siebel client is installed to the SiteScope machine and use this in the Script Path.
2. You need to 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 need to know the fully qualified path to the client executable relative to that machine.

3 You need to know the name of the Siebel applications that are available in your network. For example, call center, sales, and so on.

4 You need to 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.

5 You need to 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.

6 You need to 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.

7 For monitoring Siebel processes, SiteScope needs credentials/authorization to access the target Siebel machine. You might 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 might be that the process metrics read operation is taking too long and SiteScope is timing out. In this case you might want to specify an appropriate timeout value for perfex in the Infrastructure Settings Preferences page; for example, change the **Perfix timeout** value to 120 seconds. To access the Infrastructure Settings Preferences, expand **Preferences** in the left menu tree, choose **Infrastructure Settings Preferences**, and select the **General Settings** section.

8 You need to know the full path to the executable directory of the Siebel Server Manager Client relative to the machine it is installed on.

9 You need to make sure that the Siebel Server Manager Client's libraries are available to the Client. This varies according to the platform on which SiteScope is running:

- **For SiteScope on Solaris/Linux.** If the client libraries are installed locally, you need to explicitly configure the LD_LIBRARY_PATH to include the directory containing the Siebel Server Manager Client's libraries (for example, /var/siebel/client/lib).

  If you are running the Siebel Server Manager Client locally on the SiteScope server, update the LD_LIBRARY_PATH line in the <**SiteScope install path**>**/SiteScope/classes/start-monitor** script.

  If you are accessing the Siebel Server Manager Client on a remote server, you need to have a remote UNIX server profile to connect to that server. 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

- **For SiteScope on Windows.** If the client libraries are installed locally, you need to add a system variable called LD_LIBRARY_PATH that includes the path to the bin directory of the Siebel Client Manager.

  If you are accessing the Siebel Server Manager Client on a remote server, you need to have a remote NT server profile to connect to that server (NetBIOS connections only). Enter the full path to the Siebel Server Manager executable directory relative to the server chosen in the **Script Path** field on the Choose Server page.

Configuring This Monitor

For details on configuring this monitor, see “Siebel Application Server Monitor Settings” on page 664.

Siebel Log File Monitor Overview

The Siebel Log File Monitor is used for automatically scanning multiple log files for detailed data and 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 might have otherwise been unaware of until something more serious happened.

Note: The Siebel Log File Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

Each time the Siebel Log File Monitor runs, it examines only those log entries added since the last time it ran.

Each time that it runs this monitor, SiteScope starts from the point in the file where it stopped reading last time it ran. This insures that you are only notified of new entries and speeds the rate at which the monitor runs.

Note: This behavior can be overridden but is not recommended and should only be done for troubleshooting purposes.

Scheduling This Monitor

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.

Configuring This Monitor

For details on configuring this monitor, see “Siebel Log File Monitor Settings” on page 667.

Siebel Web Server Monitor Overview

The Siebel Web Server Monitor allows you to use SiteScope to monitor statistical and operational information about a Siebel server by way of the Siebel Web server plug-in. You can use this monitor to watch Siebel server login session statistics and gauge the performance of the Siebel server Object Managers and database.

Note: The Siebel Web Server Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

System Requirements

The following are several key requirements for using the Siebel Web Server Monitor:

- The Siebel Web server plug-in must be installed.
- The Siebel Web server plug-in should be configured to enable the display of the statistics you want to monitor. This may require that stats page sections be enabled by editing the **eapps.cfg** file for the Siebel server. Consult the Siebel documentation for more information.

Configuring This Monitor

For details on configuring this monitor, see “Siebel Web Server Monitor Settings” on page 670.

SilverStream Server Monitor Overview

Use the SilverStream Server Monitor to monitor the server performance metrics pages for SilverStream servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SilverStream server you are running.

You need to know the server statistics URL for the SilverStream server you want to monitor. For some server configurations, you must use the server name rather than the IP address for the server.

Note: The monitor supports SilverStream versions 4.x. There is limited support for versions 5.0 and higher (includes only hits and bytes in the available counters).

For details on configuring this monitor, see “SilverStream Server Monitor Settings” on page 674.

SunONE Server Monitor Overview

Use the SunONE Server Monitor to monitor performance metrics reported in the stats-xml file of SunONE servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SunONE server you are running.

Setup Requirements for the SunONE Server Monitor

Before you can use the SunONE 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 become effective.

Configuring This Monitor

For details on configuring this monitor, see “SunONE Server Monitor Settings” on page 676.

Tuxedo Monitor Overview

Use the Tuxedo Monitor to monitor the server performance data for BEA Tuxedo servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Tuxedo server in your environment.

System Requirements

Before you can use the Tuxedo Monitor, there are a number of configuration requirements involving the Tuxedo environment. An overview follows:

- 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 need to install, configure, and enable the Tuxedo Workstation component to allow SiteScope to make requests of the Tuxedo server.
- The client and server side workstation component software versions should be the same. Some versions of the client software can work with multiple versions of Tuxedo servers but support information is limited.
- If Tuxedo 7.1 or later is installed on both the server you want to monitor and the SiteScope server, more than one Tuxedo server can be monitored at a time. If Tuxedo 6.5 or earlier is used, only one Tuxedo server can be monitored at a time.
- If SiteScope is outside the domain of the Tuxedo server, the Tuxedo Workstation client software needs to be installed on the server where SiteScope is running. This is usually is 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 need to be added to the SiteScope environment:

- %TUXDIR% should be set on the monitoring machine to the <Tuxedo_root_folder>
- <Tuxedo_root_folder>\bin should be added to %PATH% variable

Note: Any environment variables (for example, TUXDIR) should be defined as system variables, not user variables.

Configuring This Monitor

For details on configuring this monitor, see "Tuxedo Monitor Settings" on page 678.

UDDI Monitor Overview

The UDDI Monitor is designed to perform a search in the UDDI Server. Each time that the monitor is run, SiteScope checks if the UDDI Server can find a business entity.

Setup Requirements for the UDDI Monitor

The following are requirements for using the UDDI Monitor:

- The UDDI server must use UDDI Version 2.
- The administrator of the UDDI server can limit or disable this monitor.

Configuring This Monitor

For details on configuring this monitor, see "UDDI Monitor Settings" on page 680.

VMware Performance Monitor Overview

The VMware monitor is designed to monitor VMware-based servers. VMware supplies much of the virtualization software available for x86-compatible computers.

The monitor supports monitoring:

- Single VMware ESX server installations.
- ESX server clusters managed by VMware Virtual Center.
- VMotion of virtual machines.

During initial monitor creation, the new monitor uses the connection URL configured to access the software and dynamically discover the object hierarchy and available performance counters. You can select from these performance counters to determine which measurements SiteScope should retrieve for reporting server status.

For details describing all the available counters, refer to the VMware documentation available at:

http://www.vmware.com/pdf/ProgrammingGuide201.pdf

VMotion Support

VMotion is a technology from VMware which allows transparent transferring of virtual machines between physical hosts in a virtual infrastructure cluster. It allows you to move your virtual machines from one server to another without having to turn those virtual machines off. This process can be done both manually and automatically as part of cluster load-balancing.

The VMware monitor is browseable and the counters tree is designed so that virtual machine nodes are not children of physical host nodes. This means that the structure of the tree does not change during VMotion and if counters from a virtual machine are selected for this monitor, they will not change as a result of VMotion. This is regardless of where the virtual machine belonged at any particular moment.

SSL Connectivity

VMware servers are generally configured to use SSL encryption for administrative connections. This can be determined by the prefix of the Web service URL. The https:// prefix means that it is a secure, encrypted connection. Monitoring a VMware server which uses an encrypted connection, requires importing the server certificate.

To import a server certificate:

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 jssecacerts file.

3. Make a copy of <**SiteScope root directory**>**/java/lib/security/cacerts** and rename it <**SiteScope root directory**>**/java/lib/security/jssecacerts**. After doing this, manually check to make sure the **jssecacerts** file is located in the <**SiteScope root directory**>**/java/lib/security** directory. The reason for creating the **jssecacerts** file is that the default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Creating a copy with a different name allows new certificates to be imported and not be overwritten with future installations or upgrades.

Note: This step is not necessary if you already have a **jssecacerts** file.

Configuring This Monitor

For details on configuring this monitor, see “VMware Performance Monitor Settings” on page 681.

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 allows 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 BEA WebLogic Application Server monitor uses the Java JMX interface to access Runtime MBeans on the WebLogic server. An MBean is a container that holds the performance data. You must set certain permissions on the WebLogic server for SiteScope to be able to monitor MBeans.

Important: WebLogic Application Server Monitors cannot be used to monitor WebLogic 9.x servers.

- To monitor these servers, use a JMX monitor as described in "JMX Monitor Settings" on page 735.
- For further details, see "Creating a JMX Monitor for a WebLogic 9.x Server" on page 489.

If you are using a WebLogic 9.x server, the rest of this chapter is not relevant.

Configuration Requirements 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.

Configuration Requirements for Monitoring WebLogic 7.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 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. See the WebLogic server documentation for more information.

Configuring SiteScope to Use T3 Over SSL Against a WebLogic Server

You use the following steps to configure a WebLogic Monitor with the **Secure Server** option to monitor a WebLogic 7 or 8 server.

To configure SiteScope to use SSL for WebLogic server monitoring:

1. 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 need to enter this information in the WebLogic Monitor setup.
2. 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 need to 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
   ```

3. Obtain a valid BEA license file and put it somewhere on the SiteScope machine. This is the file named 'license.bea' in the BEA installation directory.

4 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/java/lib/ext** directory as this causes the Weblogic monitor to fail. You must install it in a separate directory on the server where SiteScope is running.

---

5 Open SiteScope and add a WebLogic Application Server Monitor.

6 Complete the fields in the form as indicated and as described in the following steps.

7 Select the **Secure Server** option.

8 Enter the full path to the **wlcipher.jar** and **weblogic.jar** files in the **WLCipher Jar File** and the **WebLogic Jar File** fields, respectively.

9 A valid WebLogic license file must be copied to the SiteScope server. Enter the full path to the BEA license file in the **WebLogic License File** field.

10 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 **Location of JVM** field.

11 With the other applicable fields completed, you should be able to browse the counters on the WebLogic server over SSL when you click the **Get Counters** button.

Configuring This Monitor

For details on configuring this monitor, see “WebLogic Application Server Monitor Settings” on page 684.

WebSphere Application Server Monitor Overview

Use the WebSphere Application Server Monitor to monitor the server performance statistics from IBM WebSphere servers using the performance monitoring interfaces provided with WebSphere. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate WebSphere Application Server Monitor instance for each WebSphere Application Server in your environment.

System Requirements

Before you can use the WebSphere Application Server Monitor, there are a number of configuration requirements involving the server environment. The following is an overview of the configuration steps:

For WebSphere 3.5.x and 4.x

Use the following workflow to prepare the WebSphere environment for SiteScope monitoring of WebSphere versions 3.5.x and 4.x:

- Install the IBM WebSphere Administrator's Console on the SiteScope server if you are monitoring WebSphere versions 3.5.x or 4.x.

  If installing the Administrator's Console:

  - Select **Custom Installation** option during installation.
  - Select **Administrator's Console** and **IBM JDK 1.2.2.** in the **Choose Application Server Components** dialog box.
  - Specify the machine you want to monitor during the installation.
- Enable the WebSphere servers to be monitored.
  - For WebSphere 3.5.x, enable EPM Counters on the WebSphere server.
  - For WebSphere 4.x, enable PMI Counters or enable the Performance Monitoring Service on the WebSphere server. You can enable the counters for the application you want to monitor via the WebSphere Administrator's Console.

  - For WebSphere 4.x, select **Resources** and then select the **Performance** option. In the dialog box that opens, expand the **Performance Modules** tree. To manage different levels of performance data, select the performance modules, choose a performance level, and then click the **Set** button.

- Alternatively, on WebSphere 3.5.x, you can set the EPM Specification to:

  ```
  epm=high:epm.beanMethodData=none
  ```

  by using the WebSphere Administrator's Console.

- If security has been enabled on the WebSphere server, the server security ring must be copied to the admin client.

For WebSphere 5.x

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.

To install the correct client software on a SiteScope server:

1. Install the **Administration (or admin console) Performance Analysis** option from the custom options menu in the WebSphere 5.x install.

   Important: Certain trial versions of IBM WebSphere do not include the Performance Analysis option required by the SiteScope WebSphere Application Server Monitor. The SiteScope monitor can only work when a complete WebSphere production installation is available.

2. Copy all of the files from the **lib** folder of a WebSphere 5.x Application Server installation to the **lib** folder on the client install from step 1.

3. 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.

4. You must enable the WebSphere servers to be monitored. For WebSphere 4.x and 5.x, enable PMI Counters or enable the Performance Monitoring Service on the WebSphere server. You can enable the counters for the application you want to monitor via the WebSphere Administrator's Console.

   For WebSphere 5.x, Click on **Servers** > **Application Servers**. Select the server to be monitored from the Application Server list. From the Configuration tab, click on the Performance Monitoring Service in the Additional Properties list. Click the **Start Up** check box and select the **Initial specification** level as Standard or Custom. Then click the Apply button.

5. 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.

For WebSphere 6.x

To enable monitoring WebSphere version 6.x, you must have the following directories copied onto the SiteScope machine:

- AppServer/Java
- AppServer/lib

These directories can 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. This is the recommended 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. This is the least recommended option because of the size of the application server files.

Once you have the **AppServer/Java** and **Appserver/lib** files on the SiteScope machine, use the following procedure to prepare the WebSphere environment for monitoring WebSphere 6.x.

To set up monitoring WebSphere 6.x:

1. On the WebSphere server, select **Servers** > **Application Servers** > **<server name>** > **Performance Monitoring Infrastructure (PMI)** and ensure that the counters are set to **Extended**.
2. 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.

3 Open SiteScope, add the WebSphere Application Server Monitor, and configure the settings. For details, see "WebSphere Application Server Monitor Settings" on page 687.

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.

WebSphere version 6.x supports global security. Global security is set up and maintained through the WebSphere administrative console. To enable this functionality in SiteScope, you must configure the WebSphere 6.x monitor in the Advanced Settings pane.

Configuring This Monitor

For details on configuring this monitor, see "WebSphere Application Server Monitor Settings" on page 687.

WebSphere MQ Status Monitor Overview

Use the WebSphere MQ Status Monitor to monitor the performance attributes of MQ Objects: channels and queues, on MQ Servers v5.2 and above (formerly known as MQSeries). You can monitor both performance attributes and events for channels and queues.

Note: The WebSphere MQ Status Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

You can set the error and warning thresholds for the WebSphere MQ Status Monitor on as many as fifteen function measurements.

Software Prerequisites

This monitor requires two IBM MQ SupportPacs to be downloaded from the IBM Web site and installed on the same machine where the SiteScope server is running:

- **MA88.** MQSeries classes for Java, version 5.2.2 (5648-C60) or later. Go to the IBM Web site for this support package. Note that in some cases this component may already be bundled with the IBM MQ Server installation. Check your IBM MQ install documentation for details.
- **MS0B.** WebSphere MQ Java classes for PCF. Go to the IBM Web site for this support package.

Follow the instructions for installing both support packs. Copy the following files from these installations to <**SiteScope install path**>\SiteScope\java\lib\ext directory:

- com.ibm.mq.jar
- com.ibm.mq.pcf.jar
- connector.jar

After installing the required libraries, stop and restart SiteScope.

Channel Status Codes

You can choose from two different reporting schemes for Channel Status Code values:

- **IBM MQ Native Coding Scheme.** Report the actual or original channel status codes as documented in the IBM MQ literature.
- **HP Coding Scheme.** Report channel status codes in ascending values that are directly proportional to the health of the channel. That is, SiteScope reports a channel status value from 0 (least healthy) to 6 (healthiest). This scheme is consistent with how other HP products report MQ channel status codes. However this scheme provides less gradients than the IBM scheme, as shown in the table below:

MQ Channel Status	MQ Coding Scheme	HP Coding Scheme
Stopped	6	0
Paused	8	0
Inactive	-1	0
Initializing	4	1
Stopping	13	1
Starting	2	2
Retrying	5	3
Requesting	7	4
Binding	1	5
Running	3	6
Stopped	6	0

You can select the desired coding scheme in the **Channel Status Code Scheme** field under the Advanced Settings section.

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 disabled in the MQ server. For SiteScope to monitor these events, enable the MQ server to generate these events. A MQSC command must be issued on each queue and for each event to be enabled. In addition, appropriate 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 Monitor definition page), 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 feature has been built into this monitor to invoke a user-developed, client-side security exit written in Java.

To use this feature, specify the fully-qualified class name of the security exit component in file **SiteScope\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 the **<SiteScope install path>\SiteScope\java\lib\ext** directory. You can only deploy one security exit class for a SiteScope instance, and every MQ monitor running on that instance invokes that security exit.

In the case of a Windows-based SiteScope instance monitoring a Windows-based MQ server, the default authentication scheme requires that SiteScope be running under a user account that is recognized by the target server's Windows security group. Specifically, the SiteScope user must be added to the server's mqm group.

For information on MQ security exits and other authentication schemes, consult the IBM WebSphere MQ documentation.

Configuring This Monitor

For details on configuring this monitor, see “WebSphere MQ Status Monitor Settings” on page 691.

WebSphere Performance Servlet Monitor Overview

The WebSphere Performance Servlet Monitor monitors the server performance statistics for IBM WebSphere servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate WebSphere Performance Servlet Monitor instance for each WebSphere Application Server in your environment.

System Requirements

The following are several key requirements for using the WebSphere Performance Servlet Monitor:

- The WebSphere Performance Servlet is an optional component for WebSphere 3.0x and 3.5x versions. The performance servlet must be installed on WebSphere servers to use this monitor. A patch needs to be applied according to which WebSphere 3.x version you are monitoring.
- The WebSphere Performance Servlet must be installed on each WebSphere 3.x server you want to monitor. The files should be copied to the **hosts\default_host\default_app\servlets** subdirectory on each WebSphere server machine. The files needed per version are as follows:

Version	Files
3.02	xml4j.jar performance.dtd perf.jar
3.5	perf35.jar
3.5.2, 3.5.3	perf35x.jar

- The WebSphere Performance Servlet should be included as part of WebSphere 4.0 although it needs to 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.Performance
  Servlet

Configuring This Monitor

For details on configuring this monitor, see "WebSphere Performance Monitor Settings" on page 693.

26

Database Monitors

This chapter includes information about monitoring 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.

DB2 Monitor Overview

Use the DB2 Monitor to monitor DB2 servers for availability and proper function. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate DB2 Monitor instance for each IBM DB2 server in your environment.

Setup Requirements for the DB2 Monitor

The following are several key requirements for using the DB2 Monitor:

- The DB2 client files and libraries must be copied to the machine where SiteScope is running. The DB2 client Control Center must be installed on the SiteScope server.
- In the DB2 Control Center console, the system you want to monitor must be added to the **Systems** list. In Add System dialog box, enter the information required:
  - **System Name: <db2_server_name>**
  - **Remote Instance:DB2**
  - **Host Name: <db2_server_name>**
  - **Service Name: <db2_server_port>** (the default is port 50000)

  Click **Retrieve** and then click **OK**.
- A remote DB2 instance needs to be added to the <**db2_server_name**> node in the Control Center Console. Select the <**db2_server_name**> node and select to add and Instance. Enter the information required in the dialog box:
  - **Remote Instance: DB2**
  - **Instance Name:<database_name_used_for_DB2_monitor>**
  - **Host Name: <db2_server_name>**
  - **Service Name: <db2_server_port>** (the default is port 50000)

  and then click **OK**.

Configuring This Monitor

For details on configuring this monitor, see “DB2 Monitor Settings” on page 698.

DB2 8.x Monitor Overview

Use the DB2 Monitor to monitor DB2 servers for availability and proper functioning. You can monitor multiple parameters or counters with a single monitor instance. This allows 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.

Setup Requirements for the DB2 8.x Monitor

The following are several key requirements for using the DB2 8.x Monitor:

- JDBC drivers for connecting to the DB2 Database server. These can be found in your DB2 server installation directories. You must use the following files: db2jcc_license_cu.jar, db2jcc_license_cisuz.jar, db2jcc.jar.
- This monitor uses the Snapshot mirroring functionality supported by DB2. You must enable the Snapshot Mirror on your DB2 instance to retrieve counters. See the following information from the IBM DB2 documentation http://www-128.ibm.com/developerworks/db2/library/techarticle/dm-0408hubel/.

Configuring This Monitor

For details on configuring this monitor, see “DB2 8.x Monitor Settings” on page 700.

Database Counter Monitor Overview

Use the Database Counter Monitor to make SQL queries for performance metrics from any JDBC-accessible database. This monitor provides optional support for calculating deltas and rates for metrics between monitor runs. You can monitor multiple counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning.

Note: The Database Counter Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

Setup Requirements for the Database Counter Monitor

The following are several key requirements for using the Database Counter Monitor:

- You must have a copy of the applicable JDBC database driver file (for example, the Oracle thin driver is packaged in a file called classes12.zip) on the SiteScope server. Copy the downloaded driver file into the **<SiteScope install path>/WEB-INF/lib** subdirectory. If the file is in zip format, do not unzip the file. Stop and restart the SiteScope service after copying the driver file to the SiteScope machine.
- You need to know the syntax for accessing the database driver. Examples of common database driver strings are:
  - **sun.jdbc.odbc.JdbcOdbcDriver.** JDBC-ODBC Bridge Driver from Sun Microsystems.
  - **com.inet.tds.TdsDriver.** TDS driver from i-net Software for Microsoft SQL databases. This driver is deployed with SiteScope.
  - **com.inet.ora.OraDriver.** A driver from Oracle for Oracle databases. This driver is deployed with SiteScope.

  - **com.mercury.jdbc.sqlserver.SQLServerDriver.** DataDirect driver from DataDirect Technologies. It is an alternative to the TDS driver for those Microsoft SQL databases that use Windows NT authentication. This driver is deployed with SiteScope.
  - **oracle.jdbc.driver.OracleDriver.** JDBC thin driver for Oracle 7 and 8 databases. This driver is an Oracle product and is supplied by Oracle.
  - **org.postgresql.Driver.** The database driver for the Postgresql database.

- You need to know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers.

  Examples of common database connection URLs are:

  - **jdbc:odbc:<dsname>**
    where <dsname> is the data source name in the system environment or configuration
  - **jdbc:inetdae:<hostname>:<port>**
    where <hostname> is the name of the host where the database is running and <port> is the port on which the database interfaces with the driver.
  - **jdbc:mercury:sqlserver://<hosthost>:1433;DatabaseName=master;AuthenticationMethod=type2**
    where <hostname> is the name of the host where the database is running.
  - **jdbc:oracle:thin:@<hostname>:<port>:<dbname>**
    where <hostname> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <dbname> is the SID of the Oracle database instance.
  - **jdbc:postgresql://<hostname>:<port>/<dbname>**
    where <hostname> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <dbname> is the name of the Postgresql database.

- Generally, you should only have one instance of each type of JDBC driver client installed on the SiteScope machine. If there is more than one instance installed, SiteScope may report an error and be unable to connect to the database. For example, installing two **classes12.zip** files from two different versions of Oracle is unlikely to work.
- You must have a database user login that SiteScope can use to access the database. SiteScope is only able to execute the SQL queries that this user has permission to execute 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, since the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.

Configuring This Monitor

For details on configuring this monitor, see “Database Counter Monitor Settings” on page 704.

Database Query Monitor Overview

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. The other reason to monitor database queries is so you can find 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. If not, the bottleneck is probably somewhere else in the network.

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 need to 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 may also choose to 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 for the Database Query Monitor

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 appropriate SiteScope directory location.

Many database driver packages are available as compressed (zipped) archive files or.jar files. Copy the downloaded driver file into the **<SiteScope root directory>/WEB-INF/lib** subdirectory. Do not unzip the file.

- You need to know the syntax for accessing the database driver. Examples of common database driver strings are:
  - **sun.jdbc.odbc.JdbcOdbcDriver.** JDBC-ODBC Bridge Driver from Sun Microsystems.
  - **com.inet.tds.TdsDriver.** TDS driver from i-net Software for Microsoft SQL databases. This driver is deployed with SiteScope.
  - **com.inet.ora.OraDriver.** A driver from Oracle for Oracle databases. This driver is deployed with SiteScope.
  - **com.mercury.jdbc.sqlserver.SQLServerDriver.** Datadirect driver from DataDirect Technologies. It is an alternative to the TDS driver for those Microsoft SQL databases that use Windows NT authentication. This driver is deployed with SiteScope.
  - **oracle.jdbc.driver.OracleDriver.** JDBC thin driver for Oracle 7 and 8 databases. This driver is an Oracle product and is supplied by Oracle.
- You need to know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers.

  Examples of common database connection URLs are:
  - **jdbc:odbc:<dsname>**
    where <dsname> is the data source name in the system environment or configuration
  - **jdbc:inetdae:<hostname>:<port>**
    where <hostname> is the name of the host where the database is running and <port> is the port on which the database interfaces with the driver.
  - **jdbc:mercury:sqlserver://<hosthost>:1433;DatabaseName=master;AuthenticationMethod=type2**
    where <hostname> is the name of the host where the database is running.
  - **jdbc:oracle:thin:@<hostname>:<port>:<dbname>**
    where <hostname> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <dbname> is the name of the Oracle database instance.

- The database you want to monitor needs to be running, have a database name defined, and have at least one named table created in the database. In some cases, the database management software needs to be configured to allow connections via 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 need to 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 appropriate 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, since the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.

Accessing Oracle Databases Without Using ODBC

If you want to monitor an Oracle database without using ODBC, a good alternative is to use the Oracle Thin JDBC Drivers.

To set up SiteScope to use the JDBC Thin Drivers:

1. 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.

   The **Database Connection URL** format for the Oracle JDBC driver is:

   ```
   jdbc:oracle:thin:@<tcp address>:<tcp port>:<database SID>
   ```

   For example to connect to the ORCL database on a machine using port 1521 you would use:

   ```
   jdbc:oracle:thin:@206.168.191.19:1521:ORCL
   ```

Note: After the word thin is a colon (:) and an at (@) symbol.

The **Database Driver** for the Oracle thin JDBC driver is:

oracle.jdbc.driver.OracleDriver

Enter this string into the **Database Driver** text box under the Advanced Settings section of the Add Database Query Monitor form.

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", check the database SID is probably incorrect (ORCL part). This error can also occur when the tcp address, or tcp port is incorrect. If this is the case, verify the tcp port and check with the your database administrator to verify the proper SID.
- "**String Index out of range: -1**": in "Database Connection URL", check for the database server address, port, and the database SID.
- "**error, driver connect error, oracle.jdbc.driver.OracleDriver**": check syntax in item "Database Driver"
- "**error, driver connect error, oracle.jdbc.driver.OracleDriver**": check that driver is loaded in correct place
- "**error, connect error, No suitable driver**": check driver specified in item "Database Driver"
- "**error, connect error, No suitable driver**": check for syntax errors in "Database Connection URL", such as dots instead of colons

Monitoring Informix Databases

Monitoring a Informix database requires the use of a JDBC driver.

To enable SiteScope to monitor an Informix database:

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. Use your browser to add a Database Query Monitor within SiteScope.

   The **Database Connection URL** format for the Informix JDBC driver is:

   ```
   jdbc:informix-sqli://<database hostname>:<tcp port><database
   server>:INFORMIXSERVER=<database>
   ```

   If you require a username and 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, enter:

   ```
   jdbc:informix-
   sqli://pond.thiscompany.com:1526/sysmaster:INFORMIXSERVER=maindbase;
   ```

   The **Database Driver** for the Informix JDBC driver is:

   ```
   com.informix.jdbc.IfxDriver
   ```

   Enter this string into the **Database Driver** box under the Main Settings section of the Add Database Query Monitor form.

Monitoring MySQL Databases

Monitoring a MySQL database requires the use of a JDBC driver.

To enable SiteScope to monitor a MySQL database:

1. Download the MySQL JDBC driver from the MySQL web site (http://www.mysql.com).
2. Uncompress the distribution file.
3. Among all the other files, you should find a file with a .jar extension.
4. Copy the .jar file into the <**SiteScope root directory**>**/WEB-INF/lib** directory.
5. Stop and restart SiteScope.
6. Use your browser to add a Database Query Monitor within SiteScope.

   The Database Connection URL 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.

   The specification for the MySQL JDBC driver is: org.gjt.mm.mysql.Driver

   Enter this string into the **Database Driver** box under the Main Settings section of the Add Database Query Monitor form.

Possible Errors Using the MySQL Driver

If, after setting this up, you get an authorization error in the Database Query Monitor, then you may have to grant rights for the SiteScope machine to access the MySQL database. Consult the MySQL Database administrator for setting up privileges for the SiteScope machine to access the MySQL server.

Monitoring Sybase Databases

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, you should be able to find a driver in the Jconnect directory.
2. Place the zip file in th**e <SiteScope root directory>/WEB-INF/lib** directory.

Note: Do not extract the zip file.

---

3. Stop and restart the SiteScope service.
4. Add a Database Query Monitor in SiteScope.
5. For the **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
6. 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
7. For the **Database Driver**, enter:
   - com.sybase.jdbc.SybDriver (for Sybase version 4.x)
   - com.sybase.jdbc2.jdbc.SybDriver (for Sybase version 5.x)
8. Enter the database user name and password.

9. 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

10. Click **OK**.

Possible Errors with Sybase Database Monitoring

- Verify you are using the correct driver for the version of Sybase you are monitoring. Enter com.sybase.jdbc.SybDriver for Sybase version 4.x. and com.sybase.jdbc2.jdbc.SybDriver for Sybase version 5.x.
- If you get the error: "error, driver connect error, com/sybase/jdbc/SybDriver", click **Edit** for the monitor and verify that there are no spaces at the end of the driver name. Save the changes and try the monitor again.
- If you get the error: "connect error, JZ006: Caught IOException: java.net.UnknownHostException: dbservername", verify the name of the database server in the **Database Connection URL** box is correct.

Scheduling This Monitor

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 minutes.

Configuring This Monitor

For details on configuring this monitor, see "Database Query Monitor Settings" on page 709.

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. 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. If not, the bottleneck is probably somewhere else.

What to Monitor

The most important thing to monitor is the authentication of a specific user on the LDAP server. If more than one LDAP server is used, you want to monitor each of the servers.

You may also choose to monitor round trip time of the authentication process.

Status

Each time the LDAP Monitor runs, it returns a status based upon the time it takes to perform the connection.

The status is logged as either OK, warning, or error. An error status or warning status is returned if the current value of the monitor is anything other than **OK**. Errors occur if SiteScope is unable to connect, receives an unknown hostname error, or the IP address does not match the hostname.

Configuring This Monitor

For details on configuring this monitor, see “LDAP Monitor Settings” on page 715.

Oracle Database Monitor Overview

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 allows 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.

Setup Requirements for the Oracle Monitor

The following are several key requirements for using the Oracle Database Monitor:

➤ You must have a copy of the applicable Oracle JDBC database driver file (for example, classes12.zip) on the SiteScope server. Copy the downloaded driver file into the **<SiteScope root directory>/WEB-INF/lib** subdirectory. Do not unzip the file. Stop and restart the SiteScope service after copying the driver file to the SiteScope machine.

Note: More than one driver file is available for download. Some drivers support more than one version of Oracle database (for example, the classes12.zip Oracle JDBC thin driver) while others only support a particular version. If you are monitoring a recent version of Oracle database, download the latest version of the database driver.

- You must supply the correct **Database Connection URL**, a database user name and password when setting up the monitor. When using the Oracle thin driver, the database connection URL has the form of: jdbc:oracle:thin:@<tcp address>:<server name or IP address>:<database sid>.

  For example, to connect to the ORCL database on a machine using port 1521 you would use: jdbc:oracle:thin:@206.168.191.19:1521:ORCL.

  Note: The colon (:) and the at (@) symbols must be included as shown.

- You must specify the Oracle **Database Driver** that was installed on the SiteScope server when setting up the monitor. The Database Driver for the Oracle thin JDBC driver is oracle.jdbc.driver.OracleDriver.
- You should have only one version of each driver installed on the SiteScope machine. If there is more that version is installed, SiteScope may report an error and be unable to connect to the database.
- The user specified in **username** must be granted the permission to access System tablespace.

Configuring This Monitor

For details on configuring this monitor, see “Oracle Database Monitor Settings” on page 719.

SQL Server Monitor Overview

Use the SQL Server Monitor to monitor the server performance metrics pages for SQL Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each SQL Server you are running.

Setup Requirements for the SQL Server Monitor

- The SQL Server Monitor makes use of Performance Counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you need to define the connection to these servers under the Windows Remote Preferences option in the SiteScope Preferences container.
- The Remote Registry service must be running on the machine where the SQL Server is running if the SQL Server is running on Windows 2000.

Configuring This Monitor

For details on configuring this monitor, see "SQL Server Monitor Settings" on page 722.

Sybase Monitor Overview

Use the Sybase Monitor to monitor the server performance data for Sybase database servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each Sybase server in your environment.

Setup Requirements for the Sybase Server Monitor

- Before you can use the Sybase Monitor, you have to configure the Sybase server environment. The Sybase Monitor connects to the Sybase ASE server via the Adaptive Server Enterprise Monitor Server and retrieves metrics from the server using Sybase-provided libraries. When connecting to the monitored server, you connect to the Adaptive Server Enterprise Monitor Server, not the Sybase server. The Adaptive Server Enterprise Monitor Server is an application that runs on the same machine as Sybase server and retrieves performance information from the Sybase server. The Adaptive Server Enterprise Monitor Server usually has the same server name as the Sybase server, but with the suffix _ms. For example, if the name of the Sybase database application server is back-enddb, the name of the Adaptive Server Enterprise Monitor Server for that server would be back-enddb_ms.
- You also have to install the Sybase Central client on the machine where SiteScope is running to connect to the Adaptive Server Enterprise Monitor Server. The version of the client software that you install must be at least as recent or more recent than the version of the server you are trying to monitor. For example, if you have Sybase version 11.0 servers, you need to use the Sybase Central client version 11.0 or later. You also need to know the port number used to connect to the Sybase server. You can use the dsedit tool in the Sybase client console to test connectivity with the Adaptive Server Enterprise Monitor Server.

Configuring This Monitor

For details on configuring this monitor, see “Sybase Monitor Settings” on page 724.

27

Generic Monitors

This chapter includes information about monitoring various type of environment. These monitors can monitor networks, applications, and databases depending on how they are configured.

Composite Monitor Overview

Each time the Composite Monitor runs, it returns a status based on the number and percentage of items in the specified monitors and/or groups currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

One reason you should use this monitor is if you want to create complex monitor alert logic. For example, if you wanted to trigger an alert when:

- five or more monitors in a group of eight are in error
- three or more groups have monitors with errors in them
- you have two monitors, and exactly one is in error

then you could create a Composite Monitor that went into error on these conditions, and then add alerts on the Composite Monitor to take the desired actions.

If you need alert logic that is more complex than SiteScope's standard alerts allow, you may be able to use the Composite Monitor to create a customized alert behavior.

For details on configuring this monitor, see “Composite Monitor Settings” on page 726.

Directory Monitor Overview

The Directory Monitor is very useful for watching 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.

What to Monitor

Use this monitor to watch directories that contain files that may grow large enough to cause disk space problems. You can also use this to monitor directories in which new files are added and deleted frequently. A good example of the latter is an FTP directory. 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.

Scheduling This Monitor

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.

Configuring This Monitor

For details on configuring this monitor, see “Directory Monitor Settings” on page 728.

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. You can set up your File Monitors to watch for file size, setting a threshold at which you should be notified. You can even write scripts for SiteScope to execute that automatically roll log files when they reach a certain size.

What to Monitor

You can create File Monitors for any files that you want to monitor for size, age, or content. As mentioned before, you can set thresholds in SiteScope, telling it when to notify you of a problem. Log files are very good candidates for monitoring because they're prone to suddenly growing in size and crashing machines. Other files that you may want to watch are Web pages that have important content that does not change often. SiteScope can alert you to unauthorized content changes so that you can correct them immediately.

Reading and Status

Each time the File Monitor runs, it returns a reading and a status and writes them in the monitoring log file. It also writes the file size and age into the log file.

The reading is the current value of the monitor. Possible values are:

- OK
- content match error
- file not found
- contents changed

An error status is returned if the current value of the monitor is anything other than OK.

Configuring This Monitor

For details on configuring this monitor, see “File Monitor Settings” on page 730.

JMX Monitor Overview

Standard JMX remoting technology is defined by JSR 160. This standard is already supported by several software vendors and is quickly gaining acceptance.

Applications Supporting JSR 160

Here are some applications that currently support JSR 160 and information about how to monitor them:

- BEA WebLogic 9.x - Supports JSR 160, which can be enabled on the WebLogic application server by following instructions found on the BEA Web site (http://e-docs.bea.com/wls/docs90/ConsoleHelp/taskhelp/channels/EnableAndConfigureIIOP.html).

  Once enabled, the JMX URL for monitoring the server follows the following form:

  service:jmx:rmi:///jndi/iiop://<localhost>:7001/weblogic.management.mbeanservers.runtime

  where the <localhost> is the server name or IP address that is running your WebLogic application.

  For instructions to create a JMX monitor for WebLogic 9.x servers, see "Creating a JMX Monitor for a WebLogic 9.x Server" on page 489.

- Tomcat 5.x - Supports JSR 160, by defining the following properties to the JVM upon startup:
  - Dcom.sun.management.jmxremote
  - Dcom.sun.management.jmxremote.port=9999
  - Dcom.sun.management.jmxremote.ssl=false
  - Dcom.sun.management.jmxremote.authenticate=false

The above properties specify the port as 9999. This value can be changed to any available port. Also, it specifies no authentication. If authentication is necessary, see the Java Sun Web site for more details (http://java.sun.com/j2se/1.5.0/docs/guide/jmx/tutorial/security.html). If the above properties are defined when starting Tomcat 5.x on <localhost>, the following would be the JMX URL for monitoring it:

```
service:jmx:rmi:///jndi/rmi://<localhost>:9999/jmxrmi
```

Note: SiteScope 8.x runs within Tomcat 5.x, and can be monitored as described above.

- Many other vendors have recently released, or are shortly to release, versions of their software that are JSR 160 compliant, including 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).

Usage Guidelines

Use the JMX Monitor to monitor JMX statistics of a JSR 160 compliant application. 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.

The default run schedule for this monitor is every 10 minutes, but you can modify the monitor to run more or less often using the **Update every** setting.

Creating a JMX Monitor for a WebLogic 9.x Server

WebLogic 6.x, 7.x and 8.x servers can be monitored using a WebLogic Application Server monitor. For further information, see "WebLogic Application Server Monitor Overview" on page 448.

WebLogic 9.x servers cannot be monitored using a WebLogic monitor. To monitor a WebLogic 9.x server, create a JMX monitor.

To create a JMX monitor for a WebLogic 9.x server:

1 Right-click a monitor group to open the action menu.

2 Select **New Monitor.** The New SiteScope Monitor window opens.

3 Select **JMX.** The new JMX monitor window opens.

4 Enter a monitor name of your own choosing in the **Name** text box.

5 Enter the following in the **JMX URL** text box:
service:jmx:rmi:///jndi/iiop://localhost:7001/weblogic.management.mbeanservers.runtime

6 Complete the other fields as described in "JMX Monitor Settings" on page 735.

7 Click the **Get Counters** button. A tree of counters is displayed.

8 Expand the folders and select the required counters.

To help you to select the counters that you require, you can open a WebLogic monitor for versions prior to WebLogic 9.x (WebLogic 6.x, 7.x, and 8.x) and see the counters that were defined there. Search for these same counters in the counter tree. You can select additional counters that are available in the JMX monitor and were not available in the WebLogic monitors.

9 Click **OK** to save the counters and exit.

Configuring This Monitor

For details on configuring this monitor, see "JMX Monitor Settings" on page 735.

Log File Monitor Overview

Each time the Log File Monitor runs, by default, it examines only those log entries added since the last time it ran. You can change the monitor's behavior with the **Check from Beginning** property. For details, see "Check from Beginning" on page 739.

The **Run Alerts** setting controls how alerts are triggered by this monitor. If the **for each log entry matched** option is selected, then the monitor triggers alerts for every matching log entry found regardless of the defined threshold settings and the monitor status (good, warning, or error). In this way, the monitor acts much like an event forwarder. If the **once, after all log entries have been checked** option is selected, then the monitor counts up the number of matches and triggers alerts based on the **Error if** and **Warning if** thresholds defined for the monitor.

Note: Monitoring log files using SSH on Windows platforms is supported from SiteScope version 8.5 and later.

What to Monitor

The Log File Monitor is useful for automatically scanning 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 might 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 739.

Scheduling This Monitor

You can schedule your Log File Monitors to run as often as every 15 seconds. However, depending on the size of the log file, the total number of monitors you have running, and **Check from Beginning** option selected, the monitor may take 15 seconds or longer to check the file for the desired entries. The default update schedule is every 10 minutes. This is a reasonable frequency in most cases.

Configuring This Monitor

For details on configuring this monitor, see “Log File Monitor Settings” on page 737.

Script Monitor Overview

One of the primary reasons for using the Script Monitor is to integrate an existing script that you use to do a particular system management function into SiteScope. For example, if you have a script that runs a diagnostic on an application and returns a 0 reading if everything's OK, 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 e-mail or page you in the event that this monitor was in error.

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.

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 executed on the SiteScope machine. The file should be stored in the <**SiteScope install path**>/**SiteScope/scripts** directory.
Remote Script	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. 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). The monitor may fail if the appropriate exit code is not echoed back to SiteScope.
Remote Command	A script file containing a single command stored locally in the <**SiteScope install path**>/**SiteScope/scripts.remote** directory. This script file is used to run a command on a remote server. The command may be used to execute 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 upon the script that you want SiteScope to run. You can use the scheduling option to have SiteScope run scripts at different intervals throughout the week.

Status

Each time the Script Monitor runs, it returns a status and writes it into the monitoring log file. It also reports a command result, a value, and the time it took to run the command.

The command result is the exit value returned by running the command. This works for local UNIX scripts, but does not work for remote UNIX scripts, or Win NT batch files. Win NT batch file (*.bat) exit codes are not passed out of the command interpreter, and remote UNIX script exit codes are not passed back through the remote connection. See the example below for a way to receive information from the script.

Caching Script Output

The Script Monitor includes an optional feature 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
- reduce network traffic and server load by minimizing the number of times a script is executed

You can enable script output caching by entering a time value (in seconds) greater than zero in the **Cache Life** setting in the Advanced Settings section. To configure multiple Script monitors to use the data in the cache you must ensure that each monitor instance:

- is configured to use the same remote Server profile
- is configured to use the same Script file
- has a **Cache Life** value greater than zero

The **Cache Life** 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** value can be set to a value of 590 since 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 invoked 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.

Two methods exist for applying a timeout setting to Script monitors. One applies the setting as a property to an individual monitor. The second method adds the setting to groups, subgroups, or the entire SiteScope installation. The procedures for both are described below.

To set a Timeout Value for individual script monitor instances:

1. Stop the SiteScope service.
2. Using a text editor, open the SiteScope group file containing the monitor frame for the Script Monitor to which you want to apply the timeout setting.

3 Inside the Script Monitor frame (delimited by the # sign), insert a line and add the timeout setting as _timeout=time where time is replaced with the time in seconds.

4 Save the group file.

Note: Do not add blank lines, leading or trailing spaces to any record in the group file.

5 Restart the SiteScope service.

To set a Timeout Value for multiple script monitor instances:

1 Stop the SiteScope service.

2 Using a text editor, open the SiteScope group file containing one or more Script monitors to which you want to apply the timeout setting. Alternately, you can add the setting to the **SiteScope/groups/master.config** file.

3 Inside the group file frame a the top of the file before the first # symbol, insert a line and add the timeout setting as _scriptMonitorTimeout=time where time is replaced with the time in seconds.

4 Save the group file.

Note: Do not add blank lines, leading or trailing spaces to any record in the group file or master.config file.

5 Restart the SiteScope service.

Configuring This Monitor

For details on configuring this monitor, see “Script Monitor Settings” on page 742.

Web Service Monitor Overview

You use the Web Service Monitor to check the availability of a Web service accepting Simple Object Access Protocol (SOAP) requests. The Web Service Monitor checks that the service can send a response to the client in certain amount of time and to verify that the SOAP response is correct based on your selected match specifications.

The Simple Object Access Protocol is a way for a program running under one operating system to communicate with another program running under the same or different operating system (such as a Windows 2000 program talking to a Linux based program) The Simple Object Access Protocol uses the Hypertext Transfer Protocol (HTTP) and Extensible Markup Language (XML) for information exchange with services in a distributed environment.

This monitor uses a Web Services Description Language (WSDL) file to extract technical interface details about a Web service and uses information returned to create an actual SOAP request to that Web service. That is this monitor emulates a real Web service client making a request. The SOAP request can be used to confirm that the Web service is serving the expected response data and in a timely manner. The status of the Web Service Monitor is set based on the results of the SOAP request.

For more information on SOAP, refer to http://www.w3.org/TR/SOAP/.

For more information on WSDL, refer to
http://msdn.microsoft.com/xml/general/wsdl.asp.

Supported Technologies

The following specification features are currently supported:

- WSDL 1.2
- SOAP 1.1
- Simple and Complex Types based on XML Schema 2001
- SOAP binding with the HTTP(S) protocol only
- SOAP with Attachments is not supported
- Nested WSDL
- WSDL with multi-ports and multi-services

Note: The monitor does not support SOAP 1.2.

Important: 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.

Status

The status reading shows the most recent result for the monitor. It is also recorded in the SiteScope log files, e-mail alert messages, and can be transmitted as a pager alert. The possible status values are:

- OK
- unknown host name
- unable to reach server
- unable to connect to server
- timed out reading
- content match error

- document moved
- unauthorized
- forbidden
- not found
- proxy authentication required
- server error
- not implemented
- server busy

The final status result is either OK, error, or warning based on the threshold established for these conditions.

Integration with HP Business Availability Center for SOA

If SiteScope is reporting to HP Business Availability Center, the monitor sends SOA samples, in addition to the regular samples it sends, for use in HP Business Availability Center for SOA. If the **HP BAC Logging** setting is set to **Do not report to HP Business Availability Center**, the monitor does not send any samples to HP Business Availability Center.

Configuring This Monitor

For details on configuring this monitor, see “Web Service Monitor Settings” on page 748.

XML Metrics Monitor Overview

The XML Metrics Monitor operates like many other browsable monitors: it gathers information from a source, organizes it into a browsable tree structure, and allows the user to choose which items in the tree should be monitored. It works by requesting an XML file that is accessible by an URL.

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.

When defining the monitor, the XML metrics file is parsed for a list of counters. SiteScope displays a tree of counters for you to choose the metrics you want to monitor. When the monitor runs, the XML metrics file is parsed to extract values for each of the counters selected during setup.

System 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 Transform Test” on page 1412.

Configuring This Monitor

For details on configuring this monitor, see “XML Metrics Monitor Settings” on page 751.

28

Network Monitors

This chapter includes information about monitoring network health and availability.

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. Therefore, it is important that you monitor your DHCP servers to verify that they are working properly.

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.

Note: 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. See the section on Installation of DHCP Software Library below for more information.

Installation of DHCP Software Library

The SiteScope DHCP Monitor uses the jDHCP library, available from http://www.dhcp.org/javadhcp/. After downloading the library (either in .zip or in .tar.gz format), extract the file named JDHCP.jar and place it in the **<SiteScope install path>/SiteScope/java/lib/ext** directory, such that the file is located at **<SiteScope install path>/SiteScope/java/lib/ext/JDHCP.jar**. After installing the **JDHCP.jar** file, stop and restart the SiteScope service.

Scheduling This Monitor

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 frequently (every 2-5 minutes).

Configuring This Monitor

For details on configuring this monitor, see “DHCP Monitor Settings” on page 756.

DNS Monitor Overview

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. Therefore, it is important that you monitor your DNS servers to check that they are working properly.

Most companies have both a primary and a secondary DNS server. If your company employs a firewall, these 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.

Scheduling This Monitor

If your DNS servers fail, users start complaining that "everything's broken", so you should monitor them often. For example, assume that you have both a primary and secondary DNS server outside your firewall and an internal DNS server inside your firewall. Your internal server is critical, so you should monitor that one every 2 - 5 minutes. That's also a good interval for your primary DNS server that sits outside of your firewall. You can monitor the secondary DNS server less often. Every 10 or 15 minutes should be fine.

Configuring This Monitor

For details on configuring this monitor, see “DNS Monitor Settings” on page 757.

FTP Monitor Overview

If you provide FTP access to files, it is important to check that your FTP server is working properly. The FTP monitor checks FTP servers to insure the accessiblity of FTP files.

Setup Requirements

To use this monitor you need to:

- have network access to an FTP server
- know the relative paths, if any, to the files on the FTP server
- know an applicable user name and password to access the files
- know the filenames of one or more files available for FTP transfer

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. It is recommended that you check one small file and one large file.

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.

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.

Check for Content Change

Use the **Check for Content Change** option in the Advanced Settings to have SiteScope compare file contents to a previous, successful download of a file.

Unless this is set to **no content checking**, SiteScope records a checksum of the downloaded document the first time the monitor runs. The monitor then does a checksum comparison each subsequent time it runs. If the checksum changes, the monitor reports a status of **content changed error** and goes into to error.

Generally, if you want to check for content changes in a file that normally is not expected to change, you want to use the **compare to saved contents** option. This option saves a checksum baseline from the first successful download run of the monitor and compares all subsequent checksums to that baseline. The monitor continues to report an error until either the subject file is replaced with the file having the original content (checksum) or the **Check for Content Change** option is set to **reset saved contents** and the monitor is run with this setting. After running the monitor with this setting, the checksum baseline is updated and the monitor reverts back to the **compare to saved contents** option.

The **compare to last contents** option compares the checksum of the last successful download to that of the next successful download. If the checksums are different, an error is reported for that run of the monitor. The checksum from the most recent successful download then replaces the previous one. If the checksum of the next monitor run is the same as the new saved value, the monitor changes to a status of good.

Configuring This Monitor

For details on configuring this monitor, see “FTP Monitor Settings” on page 758.

Formula Composite Monitor Overview

One reason you should use this monitor is if you have devices or systems in your network that return values which you want to combine in some way to produce a composite value. The following monitor types can be used to build a Formula Composite Monitor:

- Database Query monitor. For more information see “Database Query Monitor Overview” on page 469.
- Script Monitor. For more information see “Script Monitor Overview” on page 491.
- SNMP Monitor. For more information see “SNMP Monitor Overview” on page 521.
- Windows Performance Counter Monitor. For more information see “Windows Performance Counter Monitor Overview” on page 543.

If you need alert logic that is more complex than SiteScope's standard alerts allow, you may be able to use the Formula Composite Monitor to a create custom alert behavior. For example, 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 upon the measurement results of the two subordinate monitors and the calculation specified for the composite monitor.

Notes and Limitations

- You must create at least two individual Script, SNMP, Database Query or Windows Performance Counter monitor instances before you can set up a Formula Composite Monitor for those monitors.
- The monitors you create for use with a Formula Composite monitor should be configured to return a single value per monitor. This is generally simple with SNMP monitors. Database Query and Script monitors should use queries and scripts that return a single value. For 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 Advanced 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.
- You should only use the Formula Composite monitor for calculations that you consider to be compatible data types. The monitor does not verify that the data returned by the subordinate monitors are compatible.
- You can select two different types of monitors as subordinate monitors of a Formula Composite monitor. For example, one monitor may be a Script monitor and the other may be a Database Query monitor.
- Moving any of the monitors being used by the Formula Composite Monitor causes the composite monitor to report an error. If it is necessary to move either of the underlying monitors, recreate or edit the Formula Composite Monitor to select the monitor from its new location.

Configuring This Monitor

For details on configuring this monitor, see “Formula Composite Monitor Settings” on page 762.

MAPI Monitor Overview

Use the MAPI Monitor to monitor the availability of Microsoft Exchange 5.5 and above. The monitor check for e-mail delivery time. This allows you to verify availability of the MAPI server by sending and receiving a test message in a Microsoft Exchange e-mail account. Create a separate MAPI monitor instance for each Microsoft Exchange server in your environment.

System Requirements

There are several important configuration requirements that must be performed or verified before the MAPI Monitor can be used. This section describes the steps you use to configure your environment for this monitor. The following are several definitions that are used in the steps listed below.

- **Local Administrator.** An account that has administrative privileges on the local machine. An account can have this privilege either implicitly by having Domain Admin privileges or explicitly by adding as a member of the Administrators group on the local machine. Consult your system administrator, if necessary, for help with creating accounts.
- **MailBox Owner.** This is an "owner" account for which an Exchange mailbox has been set up. To use the 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).

Before creating a MAPI Monitor, you must perform the setup steps in the e following setup steps must be performed.

Preparing the System for Using the MAPI Monitor:

Before creating a MAPI Monitor, perform the following setup steps:

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 setup page supports up to two mailboxes per Exchange Server. If only one mailbox is specified on the MAPI Monitor setup page the same mailbox can be used for the sender and receiver accounts. Consult your Exchange system administrator if you need 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 step 1, which are by definition domain logons, must be added as to the Administrators group on the SiteScope server.

➤ Click **Start** > **Settings** > **Control Panel** > **Users and Passwords** > **Advanced tab** or open the Computer Management utility and expand the **Local Users and Groups** folder in the left pane and click the **Groups** folder.

➤ Double-click the Administrators group icon to open the Administrators Properties window.

➤ Click the **Add** button to add each Mailbox Owner you expect to use with the 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 in to the SiteScope server as the MailBox User created in step 1 the Outlook wizard may start for setting up an Outlook profile for the mail box. If an Outlook client is already installed, then you may run 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 if necessary.

Creating an Outlook profile is not necessary, although it may be helpful for the purpose of troubleshooting. Once the wizard prompts you to set up a profile you can cancel to exit the wizard.

5 Verify that the SiteScope user logon is a member of Administrators group or a domain administrator account.

Important: The SiteScope user account must be a Local Administrator or be a member of the domain admins group.

To change the logon account for the SiteScope user:

- Open the **Services** control utility on the SiteScope server.
- Right-click the **SiteScope** service entry and click **Properties**. The SiteScope Properties settings page opens.
- Click the Logon Properties tab.
- Verify that the SiteScope user is run as a member of Administrators group or a domain logon account. To change the logon properties, click the **This account** radio button and enter the SiteScope user logon.
- Restart the SiteScope server after making changes to the SiteScope service logon account.

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.

- ➤ Click **Start** > **Programs** > **Administrative Tools** > **Local Security Policy**. The Local Security Policy panel opens.
- ➤ Click the **Local Policies** folder in the left pane and then click the **User Rights Assignments** folder to display the list of policies.
- ➤ Double-click the **Act as part of the operating system** policy item in the right pane. The Local Security Policy Setting list opens.
- ➤ 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.
- ➤ Enter the SiteScope user logon using the **domain\logon** format if the SiteScope user is a domain account.
- ➤ 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**.
- ➤ Restart the SiteScope service after making changes to security policy.

Configuring This Monitor

For details on configuring this monitor, see “MAPI Monitor Settings” on page 765.

Mail Monitor Overview

The Mail monitor checks to see that the mail server is both accepting and delivering messages.

What to Monitor

Most companies have both a primary and a secondary mail server. At companies that employ a firewall, there may even be a third, internal, mail server. Each of these servers should be monitored regularly.

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.

Scheduling This Monitor

It is a good idea to monitor your primary mail server at least every five minutes. The other mail servers can be monitored less often. You may find it useful to set up a special mail account to receive the test e-mail messages send by SiteScope.

Configuring This Monitor

For details on configuring this monitor, see “Mail Monitor Settings” on page 768.

Network Bandwidth Monitor Overview

The Network Bandwidth Monitor operates like many other browsable monitors to gather information from a source and allow 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/templates.mib/** are used to create a browsable tree that contains names and descriptions of the objects found during the traversal. Note that an object may or may not be displayed with a textual name and description, depending on the MIB's available in SiteScope/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.

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, edit the <**SiteScope root directory**>**/groups/master.config** file and change the value of the **_performNetworkBandwidthSanityCheck=true** property to false (=false).

Configuring This Monitor

For details on configuring this monitor, see "Network Bandwidth Monitor Settings" on page 773.

Ping Monitor Overview

The network can often be a Web traffic bottleneck, especially on relatively slow wide area network connections. 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

It is recommended that you set up monitors that test your connection to the Internet at several different points. For example, if you have a T1 connection to a network provider who in turn has a connection to the backbone, you would want to set up a Ping Monitor to test each of those connections. The first monitor would ping the router on your side of the T1. The second would ping the router on your provider's side of the T1. The third monitor would ping your provider's connection to the backbone.

In addition to these monitors, it is also a good idea to have a couple of other monitors ping other major network providers. These monitors do not really tell you whether the other provider is having a problem, but it does tell you if your network provider is having trouble reaching them.

Scheduling This Monitor

You can monitor your own router as often as every 2 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.

Configuring This Monitor

For details on configuring this monitor, see “Ping Monitor Settings” on page 778.

Port Monitor Overview

The Port Monitor is useful for monitoring network applications that none of the other SiteScope monitors watch. You are notified immediately if SiteScope is unable to connect to the monitored port.

What to Monitor

You can use the Port Monitor to watch those network applications that SiteScope does not specifically watch, such as Gopher and IRC services, some media services, or other custom network applications.

Scheduling This Monitor

Scheduling Port monitors depends on the application or system you are monitoring. The Port Monitor does not use many resources, so you can schedule it to run as often as every 15 seconds if necessary. Monitoring most systems every 10 minutes is normally sufficient.

Status

Each time the Port Monitor runs, it returns 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 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.

Configuring This Monitor

For details on configuring this monitor, see “Port Monitor Settings” on page 779.

RTSP Monitor Overview

You use the RTSP Monitor to check the availability of a media source or media file, check that it can be retrieved, that the file is complete, and that the download rate meets your requirements.

Note: The RTSP Monitor does not support Real Media file types (for example: *.ra, *.ram files) or Windows Media files (for example: *.asf files). Use the Real Media Server Monitor and Real Media Player Monitor or the Windows Media Server Monitor and Windows Media Player Monitor to monitor these types of services. For more information see “Stream Monitors” on page 549.

Solaris and Linux Requirements

For SiteScope on Solaris or Linux, the RTSP Monitor requires that an X11 server be available. If SiteScope is unable to contact the X11 server specified by the DISPLAY environment variable, it cannot load the JMF player used by this monitor and issues a "**Player Create Error** error message.

The DISPLAY environment variable must be set prior to starting SiteScope. For convenience, this variable can be set in the SiteScope user's login environment scripts.

The following are three options for meeting the configuration requirement for the RTSP Monitor on Solaris and Linux:

➤ Log in to the graphical system console, execute xhost +localhost, and set your DISPLAY variable to the appropriate value before starting SiteScope.

You must remain logged into the graphical console to maintain the X11 server active. If you log out of the console session, the X11 server shuts down and the RTSP Monitor is not able to contact it.

- Run a PC X11 server, such as Exceed, and specify the appropriate value for DISPLAY prior to starting SiteScope.

  The X11 server process (such as Exceed), must be running as long as SiteScope is running. If the RTSP Monitor is unable to contact the X11 server it generates a Player Create Error message.

- Install and run Xvfb, the X Virtual Frame Buffer on your Solaris/Linux system. Xvfb is an X11 server emulator which can be run as a daemon and meets the X11 server requirements of the RTSP Monitor.

  Most Linux distributions include Xvfb, and it is also available on Solaris 9. For earlier Solaris versions, you need to download the X11R6 source code from ftp.x.org.

  After installing Xvfb, a startup script can be configured to start Xvfb on system boot with a command similar to the following:

  ```
  /path_to_xvfb/Xvfb:77 > /dev/null 2>&1 &
  ```

  The **:77** parameter tells Xvfb to run on display number 77. In this example, we would need to set our display variable to <hostname>:77.

  The advantage of Xvfb over the other two options is that it provides a working X11 server without requiring that a user be logged into a system console on either an NT or UNIX system.

The RTSP Monitor makes use of the Java Media Framework (JMF) which provides the capability of monitoring a variety of real time digital media types and protocols. This includes HTTP retrieval of media files and RTSP streaming of many types of files. The table below is an overview of the media formats that have some support in the RTSP Monitor.

Note: Due to the many variations of media recording options, not all files of the types listed below are supported by the Java Media Framework and RTSP Monitor. For example, some MP3 and MOV options are not supported. We recommend that you test a variety of files with the RTSP Monitor to determine if the file format you want to monitor can be decoded by the RTSP Monitor.

Media Type	**File Format**
Audio Interchange File Format (Apple)	***.aiff**
Audio Video Interleave (Microsoft)	***.avi**
Flash (Macromedia)	***.swf, *.spl**
Global Standard for Mobile Communications GSM (wireless telephony standard)	***.gsm**
HotMedia (IBM)	***.mvr**
Musical Instrument Digital Interface (MIDI)	***.mid**
Motion Picture Experts Group MPEG-1 Video	***.mpg**
MPEG Layer II Audio	***.mp2**
MPEG Layer III Audio	***.mp3**
QuickTime Movie (Apple)	***.mov**
Sun Audio (Sun Microsystems)	***.au**
Wave audio file format (Microsoft)	***.wav**

A more complete list of supported media types can be found at http://java.sun.com/products/java-media/jmf/2.1/formats.html#RTPFormats.

Note: The SiteScope RTSP Monitor does not support RealMedia formats from RealNetworks. To monitor RealMedia servers and media formats, see the Real Media Server Monitor or Real Media Player Monitor in "Stream Monitors" on page 549.

Scheduling This Monitor

This monitor should be set to run according to your reasonable acceptable error period. The utilization of monitoring bandwidth and overall monitoring system performance should be considered in setting the run interval for this type of monitor. The default run interval is set to 10 minutes.

Status

Each time a RTSP Monitor runs, it attempts to open and read a specified media stream or download and play a specified media file. The monitor records a status and stream or file statistics when the session is completed. If the file or stream is not supported or is unavailable, an error is reported.

Each time the monitor runs it returns a status which includes the current value of the monitor. The possible status values are:

- OK
- warning
- error

The final status result is either OK, error, or warning based on threshold established for these conditions.

Configuring This Monitor

For details on configuring this monitor, see "RTSP Monitor Settings" on page 781.

SNMP Monitor Overview

Use the SNMP Monitor to monitor devices that communicate with the SNMP protocol, such as firewalls, routers, and UPS's. Several operating systems suppliers also provide SNMP agents and Management Information Bases (MIB's) for accessing workstation or server performance metrics, interface statistics, and process tables via 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 OID that maps to that value. If your router supports SNMP, for example, you could have SiteScope monitor for packet errors, bandwidth, or device status.

Note: To have SiteScope listen for SNMP traps from multiple devices, use the SNMP Trap Monitor.

Requirements for the SNMP Monitor

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 (MIB's) and configured to read those MIB's.
- You need to 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. The monitor supports monitoring agents of SNMP versions 1, 2, and 3. 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 might be helpful if you want to reach one of the SNMP table columns.

For information on relating to monitoring SNMP systems, refer to the SiteScope Knowledge Base (http://support.mercury.com).

Configuring This Monitor

For details on configuring this monitor, see “SNMP Monitor Settings” on page 783.

SNMP Trap Monitor Overview

Note: To have SiteScope query a specific device for a specific value, use the SNMP Monitor.

The SNMP Trap Monitor is useful 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 might 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.

You also need to configure the network devices to send SNMP Traps to SiteScope. On Windows 2000 systems, this can be configured via the **Administrative Tools** > **Services** > **SNMP Service** > **Properties** > **Traps** page. SNMP agents on UNIX platforms usually require that you edit the configuration files associated with the agent. For an example of working with other devices, see the instructions on the Cisco Web site for SNMP Traps and Cisco Devices.

Note: The SNMP Trap Monitor uses port 162 for receiving traps. If another application or process on the machine where SiteScope is running has bound this port, the monitor reports an **Address in use** error.

For details on configuring this monitor, see "SNMP Trap Monitor Settings" on page 787.

SNMP by MIB Monitor Overview

The SNMP by MIB Monitor gathers information from a source, organizes it into a browsable tree structure, and allows 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 MIB's implemented by the agent. Thus, you do not need to know which objects are present on the agent in advance. The monitor supports agents of version 1, 2, and 3.

The MIB files in **SiteScope/templates.mib** are then used to create a browsable tree that contains names and descriptions of the objects found during the traversal. Note that an object may or may not be displayed with a textual name and description, depending on the MIB's available in **SiteScope/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.

Troubleshooting MIB Compilation

As mentioned above, you can add to the MIBs of which SiteScope is aware by putting new MIB files in the templates.mib directory. To recompile any new MIBs, you must restart SiteScope. Unfortunately, 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. Below is a series of steps you can follow when compiling new MIBs and troubleshooting compilation failures:

- 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.
- Restart SiteScope.
- Proceed as if to add a new SNMP by MIB Monitor. Before adding the monitor, check to see that your new MIB files are listed in the MIB File drop-down box. If they are, then they were successfully compiled and you may now 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, then proceed to the next step.
- Open the file **error.log** in the logs directory. Look for error messages about MIB compilation near 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.
- Correct the errors found in **error.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 **error.log**. There is a lot of information about these errors on the Web.
- After correcting the errors described in **error.log**, restart SiteScope and follow the procedure above to verify that the new MIB files compiled correctly.

Note:

- To check compilation of the new MIB, you can also use the command line tool, which is located in **<SiteScope root directory>/tools /SNMPMIBCompilation**. This tool enables you to check the new MIB compilation, so that you do not need to restart SiteScope for every change you make in the MIB file. The directory also contains a **ReadMe** file which explains how to use the tool.
- 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. The different compilers have different behaviors. Some are more restrictive than others.

Configuring This Monitor

For details on configuring this monitor, see “SNMP by MIB Monitor Settings” on page 790.

Windows Dial-up Monitor Overview

Because the Windows Dial-up Monitor uses Remote Access, which affects the entire machine's network connectivity when it establishes a connection, it should be used on a machine that is not used for accessing resources outside of the local network. For example, if you were using a Web browser on the machine where SiteScope was running a Windows Dial-up Monitor, and the Windows Dial-up Monitor had connected, all the requests by the browser out to the Internet would also use the dial-up connection, affecting the speed of the browser and the reading from the Windows Dial-up Monitor. The 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 Windows Dial-up Monitor is completed). No two Windows Dial-up Monitors are run at the same time.

The Windows Dial-up Monitor uses the dial-up connection only for requests outside of the local network. Therefore, if you have monitors that access network resources on the local network, their readings are the same as if the 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 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.

To set up the Remote Access Service on a Windows NT machine, go to the Network Control Panel, and add the service. At that time you also have the option of adding one or more modems as Remote Access modems. At least one of the modems has to have dial out capability for this monitor to work.

You can use the Windows Dial-up Monitor to measure the performance of your Internet applications from a dial-up user's perspective. The Windows Dial-up Monitor can also be used to monitor the availability and performance of remote access servers.

What to Monitor

If you are primarily interested in dial-up availability, then you can just have the 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 dialup user, then running a suite of monitors that represent typical user tasks gives you more complete assessment.

Scheduling This Monitor

Because the Windows Dial-up Monitor stops other monitors from running while it is connected, 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 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 Windows Dial-up Monitor can run at a time, so if you have more than one Windows Dial-up Monitor, take that into account when scheduling the monitors.

Status

Each time the 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 Windows Dial-up Monitors saves the total time taken (to connect and run the monitors), the connect time (the time for the modem to establish a physical connection), the authorization time (the time after physical connection is established before the connection can actually be used), and the percentage of the monitors run that were OK.

Configuring This Monitor

For details on configuring this monitor, see “Windows Dial-up Monitor Settings” on page 793.

29

Server Monitors

This chapter includes information about monitoring server health and availability.

Browsable Windows Performance Counter Monitor Overview

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. For example, 1.24 Interrupts/sec. 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 upon this count.

Note:

- The Browsable Windows Performance Counter Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- This monitor can only be added by deploying a Solution template or SiteScope Health. For information on using templates to deploy monitors, see “Using SiteScope Templates” on page 1039.

For details on configuring this monitor, see “Browsable Windows Performance Counter Monitor Settings” on page 796.

CPU Utilization Monitor Overview

When CPU usage becomes too high, clients and customers either find that the system response has become very slow, or if applications hang as a result of high CPU usage, they simply cannot access it. Therefore, it is very important to monitor CPU usage and do something about high usage before it results in outages or poor response times.

Whether the servers in your infrastructure are running with a single CPU or with multiple CPUs, you only need to create one CPU monitor per remote server. If you have multiple CPUs, SiteScope reports on the average usage for all of them, as well as each individual CPU usage.

Scheduling This Monitor

In general, the CPU Monitor does not need to be run as often as some of the other monitors. If you do not usually suffer from CPU problems, you can run it less frequently - perhaps every half hour or so. If you are prone to CPU usage problems, you should run it more frequently. All machines have short spikes of CPU usage, but the primary thing that you are looking for is high usage on a regular basis. This indicates that your system is overloaded and that you need to look for a cause.

Status

The Status reading is the current value returned by this monitor; for example, 68% used. SiteScope displays an average for multiple CPU systems. On NT, this is the average CPU usage between runs of the monitor. On UNIX, this is the instantaneous CPU when the monitor runs.

The status is logged as either OK or warning. A warning status is returned if the CPU is in use more than 90% of the time.

Configuring This Monitor

For details on configuring this monitor, see “CPU Utilization Monitor Settings” on page 798.

Disk Space Monitor Overview

Running out of disk space can cause many problems both large and small, and it is something that can happen slowly over time or very rapidly. Having SiteScope verify that your disk space is within acceptable limits can save you from a crashed system and corrupted files.

Scheduling This Monitor

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 can specify both warning and error thresholds so that SiteScope can notify you of a potential problem in time for you to do something about it. You may even want to have SiteScope execute a script (using a Script Alert) that deletes all files in certain directories, such as /tmp, when disk space becomes constrained.

Configuring This Monitor

For details on configuring this monitor, see “Disk Space Monitor Settings” on page 800.

Exchange 2003 Mailbox Monitor Overview

The Exchange 2003 Mailbox Monitor displays important statistics about mailboxes, including mailboxes that are over a certain size, and mailboxes that have not been accessed in some number of days.

Note:

- The Exchange 2003 Mailbox Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- This monitor can only be added by deploying an Exchange Solution template. For information on using templates to deploy monitors, see “Using SiteScope Templates” on page 1039.

Scheduling This Monitor

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. The results of each execution are saved and later viewable through the Usage Stats link.

Note: 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".

Configuring This Monitor

For details on configuring this monitor, see “Exchange 2003 Mailbox Monitor Settings” on page 802.

Exchange 2003 Public Folder Monitor Overview

The Exchange 2003 Public Folder Monitor displays statistics such as access times, empty folders, folder sizes, and folders not accessed within some time period.

Note:

- The Exchange 2003 Public Folder Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- This monitor can only be added by deploying an Exchange Solution template. For information on using templates to deploy monitors, see “Using SiteScope Templates” on page 1039.

Scheduling This Monitor

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. The results of each execution are saved and later viewable through the Usage Stats link.

Note: 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".

Configuring This Monitor

For details on configuring this monitor, see “Exchange 2003 Public Folder Monitor Settings” on page 805.

Exchange 2000/2003 Message Traffic Monitor Overview

The Exchange 2000/2003 Message Traffic Monitor displays important statistics about messages handled by an Exchange 2000/2003 server, such as a count of messages sent that are larger than a certain size, or sent to a large number of recipients.

Note:

- The Exchange 2000/2003 Message Traffic Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- This monitor can only be added by deploying an Exchange Solution template. For information on using templates to deploy monitors, see “Using SiteScope Templates” on page 1039.

Scheduling This Monitor

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. The results of each execution are saved and later viewable through the Usage Stats link.

Note: 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".

Configuring This Monitor

For details on configuring this monitor, see “Exchange 2000/2003 Message Traffic Monitor Settings” on page 807.

Exchange 5.5 Message Traffic Monitor Overview

The Exchange 5.5 Message Traffic Monitor displays important statistics about messages handled by an Exchange 5.5 server, such as a count of messages sent that are larger than a certain size, or sent to a large number of recipients.

Note:

- The Exchange 5.5 Message Traffic Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.
- This monitor can only be added by deploying an Exchange Solution template. For information on using templates to deploy monitors, see “Using SiteScope Templates” on page 1039.

Scheduling This Monitor

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. The results of each execution are saved and later viewable through the Usage Stats link.

Configuring This Monitor

For details on configuring this monitor, see “Exchange 5.5 Message Traffic Monitor” on page 809.

IPMI Monitor Overview

The Intelligent Platform Management Interface (IPMI) provides an interface for reporting on device operations such as whether fans are turning and voltage flowing within server hardware. This is becoming an important part of IT system management. You use the IPMI Monitor to monitor server and network element platforms to get a more complete view of component health in business critical IT infrastructures.

You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch key operational factors that can seriously impact availability and degrade performance. Create a separate monitor instance for each server you are running.

System Requirements

The following are requirements for using the IPMI Monitor:

- The device you want to monitor has to be IPMI-enabled. In most cases, this means that the device must be designed for IPMI sensing and include a separate, dedicated IPMI network adapter. The monitor supports IPMI version 1.5 only.
- You need to know the IP address of the IPMI network adapter for the device you want to monitor. In many cases, this IP address is different than the IP address used for other network communication to and from the device. Use an applicable IPMI utility to query for the IP address or contact the applicable system administrator.

Configuring This Monitor

For details on configuring this monitor, see “IPMI Monitor Settings” on page 811.

Memory Monitor Overview

One of the primary factors that can affect your Web server's performance is memory. The two most important measurements to detect problems in this area are Pages per Second and Percentage of Virtual Memory Used, both monitored by the SiteScope Memory Monitor.

Each time the Memory Monitor runs, it returns a status message and writes it in the monitoring log file.

Scheduling This Monitor

In most environments, the Memory 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 the either server, managing a large number of remote connections can results in some performance problems. You use the error and warning thresholds to have SiteScope notify you if memory on a remote server starts to get low.

Common Problems and Solutions

Pages per second measures the number of virtual memory pages that are moved between main memory and disk storage. If this number is consistently high (>10 pages/sec), system performance is being affected. One solution is to add more memory. Another solution is to turn off non-critical services that are using memory, or move these services to a different machine. The SiteScope Service Monitor measures the memory usage for each service.

Percentage of Virtual Memory Used measures the percentage of memory and paging file space used. If this number reaches 100%, services that are running may fail and new ones are unable to start. Increasing the size of the paging file 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.

The SiteScope Process Detail tool, available when you click the Tools link listed in the Monitor Detail Table, can be used to view the memory used by each service. The ideal solution is to install an upgraded version of the service without the leak. An interim solution is to use the SiteScope Service Monitor to measure the service size and invoke 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 SiteScope Script alert to restart the server when memory usage is too high.

When deploying the Memory monitor on a remote UNIX machine, the monitor displays swap memory usage and not virtual memory usage. To monitor virtual memory usage, deploy the UNIX Resources monitor. For details, see “UNIX Resources Monitor Overview” on page 541.

Configuring This Monitor

For details on configuring this monitor, see “Memory Monitor Settings” on page 813.

Service Monitor Overview

The Service Monitor verifies that specific processes are listed as running, and optionally, it can also check to see how much CPU a process is using. If a 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 process to help minimize impact on other operations and downtime.

What to Monitor

You should create a service monitor for any service or process that should be running on a consistent basis. You can also create a script alert that restarts the service automatically if the service monitor in SiteScope cannot find it. The restartService.bat script, located in the <**SiteScope install path**>**/SiteScope/scripts** directory, is a template which you can customize to create a script for SiteScope to execute in the event your monitor fails.

Scheduling This 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 the either server, managing a large number of remote connections can results 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.

Status

Each time the Service Monitor runs, it returns a reading and a status message and writes them in the monitoring log file.

The reading is the current value of the monitor. For this monitor, the possible readings are:

- Running
- Not found

The status is logged as either OK or error. An error status is returned if the service is not found.

Configuring This Monitor

For details on configuring this monitor, see “Service Monitor Settings” on page 815.

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 allows you to monitor the remote server for loading, performance, and availability at a basic system level. See the list of example system measurements that can be monitored. Create a separate UNIX Resources monitor instance for each UNIX server in your environment.

The UNIX Resources Monitor queries the list of UNIX servers currently configured in the SiteScope UNIX Remote Preferences container. To monitor a remote UNIX server, you must define a UNIX Remote connection profile for the server before you can add a UNIX Resources Monitor for that server.

You can generate 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 Dashboard. For details, see “Server Centric Report” on page 359.

For details on configuring this monitor, see “UNIX Resources Monitor Settings” on page 818.

Web Server Monitor Overview

The information gathered by the Web Server Monitor gives you the ability to see how busy your Web site is. You can use this information to plan hardware upgrades and configuration changes that improve your visitor's experience.

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. See the section in SiteScope Log File Columns in the SiteScope Reference Guide for information on what data is recorded.

For details on configuring this monitor, see “Web Server Monitor Settings” on page 820.

Windows Event Log Monitor Overview

The **Run Alerts** setting controls how alerts are triggered by this monitor. If **for each event matched** is chosen, then the monitor triggers alerts for every matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error). In this way, the monitor acts much like an event forwarder. If **once, after all events have been checked** is chosen, then the monitor counts up the number of matches and triggers alerts based the **Error If** and **Warning If** thresholds defined for the monitor.

The Windows Event Log Monitor examines only log entries made 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 fields listed under Advanced Settings to specify values that must appear in the event entry for the entry to match.

When setting up SiteScope alerts for 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 Windows Event Log Monitor runs, it returns a reading and status message and writes them in the **<SiteScope install path>/SiteScope/logs/SiteScopeyyyy_mm_dd.log** file.

Status

The status for the Windows Event Log Monitor includes the number of entries examined, and the number of entries matched. If an interval is specified, the number of events in that interval is also displayed. Matched entries and interval entries can trigger alerts.

Configuring This Monitor

For details on configuring this monitor, see “Windows Event Log Monitor Settings” on page 822.

Windows Performance Counter Monitor Overview

Each time the 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 detail table for the monitor which represents the current value returned by this monitor. For example, 1.24 Interrupts/sec. The status is logged as either OK or warning. An error occurs if the counter could not be read.

For details on configuring this monitor, see “Windows Performance Counter Monitor Settings” on page 828.

Windows Resources Monitor Overview

Use the Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. This allows 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 Windows Resources Monitor instances for each remote server in your environment.

The Windows Resources Monitor makes use of Performance Counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you must define the connection to these servers under the Windows Remote Preferences option in the SiteScope Preferences container.

You can generate a Server Centric Report for the Windows Server by clicking the server name in the Target column of the row corresponding to the Windows Resources Monitor in Dashboard. For details, see "Server Centric Report" on page 359.

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 Transform Test" on page 1412.

Note: When monitoring Windows servers configured using SSH, you must use the **Direct Registry Queries** option for the **Collection Method** field in the Advanced Settings area when you configure the monitor.

Configuring the Windows Resources Monitor to Run on Windows 2003 as a Non-Administrator User

For the 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 allow 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.

To configure user account settings on SiteScope:

1. In the **Services** control panel, right-click the **SiteScope** service, and then click **Properties**. The SiteScope Properties dialog box opens.
2. Click the **Log On** tab, and configure the user account to log on using the selected non-administrator user account (domain or local account).

To configure user account settings on the remote monitored machine:

1 Check that you can access the remote machine. Perform a ping test and check DNS resolves the server name with its IP address.

It is also recommended 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.

2 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.

3 Add the domain or local user account to be used into the **Performance Monitor Users** and **Performance Log Users** local user groups.

Make sure that these groups have at least read permissions for the following registry key (and all its subkeys):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
Perflib]
```

Tip: To check read permissions, select **Start** > **Run**, and enter **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.

---

4 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\SecurePipe Servers\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.

To verify that the non-administrator user account works:

1 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.
- Launch it when logged on to the SiteScope machine with some other account through the RunAs command, which allows you to launch commands under different user account. Enter the following command:

  ```
  runas /env /netonly /user:tester "mmc.exe perfmon.msc"
  ```

  Then type the password (in this example, for the tester account), and the command is run under the tester user account.

2 After the Performance window opens, right-click in the right graph area and select **Add Counters**. The Add Counters dialog box opens.

3 Select **Choose counters from computer** and type the remote monitored machine name or its IP address in the box.

4 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.

Configuring This Monitor

For details on configuring this monitor, see “Windows Resources Monitor Settings” on page 833.

Windows Services State Monitor Overview

Use the Windows Services State Monitor to monitor the services installed and running on remote Windows servers. By default, the monitor returns a list of all of the services that are set to be run automatically on the remote server. You can filter the list of services returned by the monitor using regular expressions. The monitor displays the number of services running and related statistics along with a summary listing of the services installed on the remote server.

Note: The 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 to monitor processes on remote machines.

To use this monitor to generate event alerts, configure alert definitions associated with this monitor to alert **Once, after the condition has occurred exactly 1 times**. This is because the 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.

For details on configuring this monitor, see “Windows Services State Monitor Settings” on page 837.

30

Stream Monitors

This chapter includes information about monitoring applications that play media files and stream data.

Real Media Player Monitor Overview

Use the Real Media Player Monitor to monitor availability and delivery quality parameters for media files and streaming data compatible with RealNetworks Real Media Players. You can monitor multiple parameters or counters with a single monitor instance. This allows 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.

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.

For details on configuring this monitor, see “Real Media Player Monitor Settings” on page 842.

Real Media Server Monitor Overview

Use the Real Media Server Monitor to monitor the server performance parameters for RealNetworks Real Media Servers. You can monitor multiple parameters or counters with a single monitor instance. This allows you to watch server loading for performance, availability, and capacity planning. Create a separate monitor instance for each RealSystem Server you are running.

The Real Media Server Monitor makes use of Performance Counters to measure application server performance. SiteScope needs to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, you need to define the connection to these servers under the Windows Remote Preferences option in the SiteScope Preferences container.

The Remote Registry service must be running on the machine where the Real Media server is running if the Real Media Server is running on Windows 2000.

For details on configuring this monitor, see “Real Media Server Monitor Settings” on page 845.

Windows Media Player Monitor Overview

Use the Windows Media Player Monitor 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 allows you to report on delivery performance. Create a separate monitor instance for files or data streams that are representative of the content available from the site you want to monitor.

Note: You should only monitor video, not audio, streams with this monitor.

You must have an instance of Windows Media Player installed on the machine where SiteScope is running to use this monitor.

Performance Counters

The media player performance parameters or counters you can check with the Windows Media Player Monitor include:

- **Packet quality.** The percentage ratio of packets received to total packets.
- **Time quality.** The percentage of stream samples received on time (no delays in reception).
- **Stream count.** The packet count.
- **Stream rate.** The packet rate indicating the speed at which the clip is played: 1 is the actual speed, 2 is twice the original speed, and so on.
- **Buffering count.** The number of times the Player had to buffer incoming media data due to insufficient media content.
- **Buffering time.** The time spent waiting for sufficient media data to continue playing the media clip.
- **Interrupts.** The number of interruptions encountered while playing a media clip. This includes buffering and playback errors.
- **Packets lost.** The number of lost packets not recovered (applicable to network playback).

- **Packets recovered.** The number of lost packets successfully recovered (applicable to network playback).
- **Ratio bandwidth.** The ratio (as a percentage) of the actual bandwidth used to the recommended bandwidth.

  For example, 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%.
- **Recommended bandwidth.** The recommended bandwidth is bits per second.

  When a .wmv file is opened in Media Player, the property **bitrate** is the recommended bandwidth. This bandwidth is embedded in the stream itself.
- **Recommended duration.** The total duration of the media clip in seconds. This value is not effected by what was already played.
- **Sampling rate.** The sampling rate in milliseconds, for collecting statistics.
- **Stream max.** The maximum number of packets.
- **Stream min.** The minimum number of packets.

Configuring This Monitor

For details on configuring this monitor, see “Windows Media Player Monitor Settings” on page 847.

Windows Media Server Monitor Overview

Use the 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 allows 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 Windows Media Server Monitor makes use of Performance Counters to measure application server performance. SiteScope must 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 need to define the connection to these servers under the Windows Servers container in the SiteScope Preferences.

For details on configuring this monitor, see “Windows Media Server Monitor Settings” on page 849.

31

Web Transaction Monitors

This chapter includes information about monitoring web-based applications.

eBusiness Transaction Monitor Overview

Use this monitor to verify that an end-to-end transaction and associated processes complete properly. For example, you could use this monitor to verify that the following steps, each of which is a step in a single transaction, execute properly:

- Place an order on a Web site (Working with the URL Sequence Monitor)
- Check that the order status was updated (Working with the URL Sequence Monitor)
- Check that a confirmation e-mail was received (Mail Monitor Overview)

- Check that the order was added to the order database (Database Query Monitor Overview)
- Check that the order was transferred to a legacy system (Script Monitor Overview)

You should monitor any multi-step transaction process that causes other updates or actions in your systems. Monitor each of the actions taken to check that updates were performed properly and that actions were carried out successfully.

Using this example, you would first create the URL Sequence monitor, Mail monitor, Database monitor, and applicable Script monitor needed to verify each step of the chain. Then you would create an eBusiness Transaction Monitor and select each of these SiteScope monitors as a group in the order they should be executed. If any one monitor indicates a failure, the eBusiness Transaction Monitor reports an error.

Editing the Order of the Monitors in the Chain

By default, the Add eBusiness Transaction Monitor page lists monitor groups and individual monitors in the order they are created. To have the eBusiness Transaction Monitor invoke the chain of monitors in the proper order, they must appear in the proper order in the selection menu on the Add eBusiness Transaction Monitor page. You can do this by creating the individual monitors in the order which they should be executed. You can also use the **Reorder the monitors in this group** option on the Monitor Group page.

Scheduling This Monitor

Each time the eBusiness Transaction Monitor runs, it returns a status based upon the number and percentage of items in the specified monitors and/or groups currently reporting an error, warning, or OK status. It writes the percentages reported in the monitoring log file.

The general rule of thumb is to run these monitors every 10 minutes or so. If you have a very critical transaction process, you may want to run them more often.

Setting up Monitors for the eBusiness Chain

Before you can add an eBusiness Transaction Monitor, you need to define other SiteScope monitors that report on the actions and results of the steps in the sequence chain. Using the example from the usage guidelines above, you might create one or more URL Sequence Monitor for verifying the sequence of online actions, a Mail Monitor to confirm that an e-mail acknowledgement is sent, and a Database Query monitor to see that information entered online is logged into a database. To facilitate administration, use the following steps.

To set up a URL sequence chain monitor:

1 Create a new group that contains all the individual monitors to be included in the sequence chain.

2 Open the new monitor group.

3 Add the first individual monitor type needed to for the sequence (e.g URL Sequence Monitor).

Note: Monitors should be added in the order that they are executed in the chain. For example, create a URL Sequence Monitor which triggers an e-mail event **before** you create the Mail Monitor to check for the e-mail. See the note on reordering monitors above.

---

4 If necessary, set up the values to be passed from one monitor to another in the chain. For information about how this works see the section on passing variables between monitors below.

5 Add the other monitors for this transaction chain in the appropriate order of execution into the group.

Note: The individual monitors executed by the eBusiness Transaction Monitor should generally not be run separately by SiteScope. You should make sure that the **Update Every** setting for each of these monitors is set to zero (“0”).

---

6 Return to the SiteScope main panel.

7 Create a new group or open an existing group that contains the e-business transaction chain monitor you are creating.

8 Click **New Monitor** and select the eBusiness Transaction Monitor.

9 Complete the eBusiness Transaction Monitor configuration.

Configuring This Monitor

For details on configuring this monitor, see “eBusiness Transaction Monitor Settings” on page 852.

Link Check Monitor Overview

There is nothing more frustrating for your Web site visitors than trying to follow a broken link. Ensuring that your site is free of broken links is something that everyone knows they should do, but it is often the thing that gets moved to the bottom of the to-do list. This monitor can be set to check every link on your site, internal and external, every day, letting you know immediately which links have a problem.

Each time the Link Check Monitor runs, it returns a status and writes it in the monitoring log file. It also writes the total number of broken links, the total number of links, the total number of graphics, and the average time for retrieving a page.

What to Monitor

You should monitor the Web site for the availability of key content. This includes checking that image files and linked HTML files are accessible as referenced within the Web pages. Starting with your home page, the Link Check Monitor branches out and checks every link available on your entire site by default. If you only want it to check a portion of your site, specify the URL that links into the targeted area. You can limit the number of linked hops the monitor follows in the Advanced Settings section. Even if you are not the person responsible for Web content, you can set the monitor to run once a day and have the alerts e-mailed directly to your Web content developer.

Scheduling This Monitor

You probably only need to run the link monitor once a day to check for external links that have been moved or no longer work and internal links that have been changed. You can also run it on demand any time you do a major update of your Web site.

Configuring This Monitor

For details on configuring this monitor, see "Link Check Monitor Settings" on page 854.

URL Monitor Overview

The core function of the URL Monitor is to attempt to reach a specified Web page to verify that it can be retrieved, but it can also be used 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 the Retrieve Images or Retrieve Frames box located in the Advanced Settings section of the Add URL Monitor Form.

In addition to retrieving specific Web pages, the URL Monitor can verify that CGI scripts and back-end databases are functioning properly. You need to 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 allows you to verify that the contents of the page are correct.

The SiteScope URL Monitors provide you with end-to-end verification that your Web server is running, serving pages correctly, and doing so in a timely manner. Because it tests end-to-end, 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.

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 upon other applications to work correctly (such as pages that utilize a back-end database). The goal is to monitor a sampling of every type of page you serve to check that things are working. There is no need to verify that every page of a particular type is working correctly.

When you choose which pages to monitor, select pages with the lowest overhead. For example, if you have several pages that are generated by another application, monitor the shortest one with the fewest graphics. This puts less load on your server while still providing you with the information you need about system availability.

Scheduling This 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.

Status

Each time the URL Monitor runs, it returns a reading or 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 via 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, e-mail 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. A warning status or error status is returned if the current value of the monitor is a condition that you have defined as other than OK.

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 that you either:

- Import the server certificate as described below.
- Select the **Accept Untrusted Certs for HTTPS** option in the Advanced Settings as described in "URL Monitor Settings" on page 858.

To import a server certificate:

1. Check the certificates already in the keyStore, from the <**SiteScope root directory**>/**SiteScope/java/lib/security** directory, by entering:

   ```
   ../../bin/keytool -list -keystore cacerts
   ```

2. Import the certificate, from the <**SiteScope root directory**>/**SiteScope/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 **jssecacerts** file.

3 Make a copy of **<SiteScope root directory>/SiteScope/java/lib/security/cacerts** and rename it **<SiteScope root directory>/SiteScope/java/lib/security/jssecacerts**. After doing this, manually check to make sure the file **jssecacerts** is located in the **<SiteScope root directory>/SiteScope/java/lib/security** directory. The reason for creating the **jssecacerts** file is that the default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Creating a copy with a different name allows new certificates to be imported and not be overwritten with future installations or upgrades.

Configuring This Monitor

For details on configuring this monitor, see "URL Monitor Settings" on page 858.

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.

What to Monitor

You should use the URL Content Monitor if you need to verify multiple values (up to 10 variables) from the content of a single URL. Otherwise, the standard URL Monitor is normally used. One use for this monitor is to integrate SiteScope with other applications that export numeric data through a Web page. The content values are matched using regular expressions. The monitor includes the matched values as part of the monitor status which are written to the log. If the matched values are numeric data, the results can be plotted in a report.

Scheduling This Monitor

The frequency depends on the statistics being monitored. For most statistics, every several minutes is often enough.

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 returned as good, warning, or error dependent on the results of the retrieval, content match, and the error or warning status criteria that you select.

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 that you either:

- Import the server certificate as described below.
- Select the **Accept Untrusted Certs for HTTPS** option in the Advanced Settings as described in "URL Content Monitor Settings" on page 869.

To import a server certificate:

1. Check the certificates already in the keyStore, from the <**SiteScope root directory**>/**SiteScope/java/lib/security** directory, by entering:

   ```
   ../../bin/keytool -list -keystore cacerts
   ```

2. Import the certificate, from the <**SiteScope root directory**>/**SiteScope/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 **jssecacerts** file.

3 Make a copy of **<SiteScope root directory>/SiteScope/java/lib/security/cacerts** and rename it **<SiteScope root directory>/SiteScope/java/lib/security/jssecacerts**. After doing this, manually check to make sure the file **jssecacerts** is located in the **<SiteScope root directory>/SiteScope/java/lib/security** directory. The reason for creating the **jssecacerts** file is that the default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Creating a copy with a different name allows new certificates to be imported and not be overwritten with future installations or upgrades.

Configuring This Monitor

For details on configuring this monitor, see "URL Content Monitor Settings" on page 869.

URL List Monitor Overview

You can use the URL List Monitor to check a list of URLs without having to create a separate URL monitor for each one. For example, this is useful if you host several Web sites and simply want to see that they are each serving pages as expected. The URL List Monitor is not used to confirm links between pages (see the "Link Check Monitor Overview" on page 558) or other Web transaction processes (see "URL Sequence Monitor Overview" on page 569).

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.

What to Monitor

The URL List Monitor is useful for monitoring any set of URLs that you simply want to make sure are available over the network.

Scheduling This Monitor

This is strictly dependent upon 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.

If this happens once in awhile, it is probably not a problem. If it happens more often, there are several things you can do to resolve the issue:

- Schedule the monitor to run less frequently. If this conflicts with some other objective, use the other options.
- Reduce the **pause interval** set under the Advanced Settings. This minimizes the time it takes for the monitor to retrieve all of the URLs.
- 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.

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 that you either:

- Import the server certificate as described below.
- Select the **Accept Untrusted Certs for HTTPS** option in the Advanced Settings as described in "URL List Monitor Settings" on page 878.

To import a server certificate:

1. Check the certificates already in the keyStore, from the <**SiteScope root directory**>/**SiteScope/java/lib/security** directory, by entering:

   ```
   ../../bin/keytool -list -keystore cacerts
   ```

2. Import the certificate, from the <**SiteScope root directory**>/**SiteScope/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 **jssecacerts** file.

3 Make a copy of **<SiteScope root directory>/SiteScope/java/lib/security/cacerts** and rename it **<SiteScope root directory>/SiteScope/java/lib/security/jssecacerts**. After doing this, manually check to make sure the file **jssecacerts** is located in the **<SiteScope root directory>/SiteScope/java/lib/security** directory. The reason for creating the **jssecacerts** file is that the default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Creating a copy with a different name allows new certificates to be imported and not be overwritten with future installations or upgrades.

Configuring This Monitor

For details on configuring this monitor, see "URL List Monitor Settings" on page 878.

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, enter an account name via 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 via dynamic links or hidden input items.

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, SiteScope allows you to 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.

What to Monitor

You should monitor any multi-step Web page sequence that you have made available to general users to verify that they are available and function correctly. Web site visitors often assume that any problems they encounter are due to user error rather than system error, especially if they're not familiar with your application. By using this monitor to perform sequence testing, you can verify that users are able to successfully complete transactions.

Working with the URL Sequence Monitor

- The URL Sequence Monitor is more complex than most other SiteScope monitor types and the steps for working with the monitor are different than for other monitors. The following is an overview of key concepts and actions you use when working with the Dynamo Application Server Monitor:
  - The URL Sequence Monitor can be configured with between one to twenty steps. Each step is defined individually in a sequence of numbered entries in the interface. The steps must be initially configured in the intended sequence as the request for one step provides the content used in the following step.
  - You use the **Add Step** button to add a new step to the URL sequence. You only use the **OK** button at the bottom of the monitor properties panel after you have added all the desired steps and then you are ready to activate the monitor instance.
  - When you first configure a URL Sequence Monitor, be sure to configure the steps you want to include in the sequence before you click the **OK** button to create the 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 need to be familiar with HTML when working with this monitor.

- Many Web-based systems use session data to identify clients and track the state of a user's interaction with the server application. This session data is often sent back and forth to the client in the HTTP header or Post Data. You should be familiar with the session tracking methods used by the systems you want to monitor to effectively configure this monitor.

- Web-based sequences or transactions can be difficult to navigate when dealing with many Web pages. For example, Web pages that use many graphic images for navigation hyperlinks can present special challenges when configuring URL Sequence monitors. You need to be familiar with HTML hyperlink syntax when working with this monitor.

- The Main Settings and Advanced Settings for the Dynamo Application Server Monitor apply to the monitor in general and behave much the same as for other monitor types.

- When you first configure the URL Sequence Monitor, the HTML text content returned from the request made in one step is displayed in a folding panel a the bottom of the following Step panel. 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. See the "URL Sequence Monitor Settings" on page 881 and Client-side Programs help page for more information on dealing with Web page scripts.

Configuring the URL Sequence Monitor

The URL Sequence Monitor can be added to any SiteScope monitor group container in the monitor tree. The following are the steps you use to add a URL Sequence Monitor.

To configure a URL Sequence Monitor:

1. Add the URL Sequence Monitor to a monitor group container. For details, see "Configuring New SiteScope Monitor" on page 615.
2. Enter a **Name** and **Frequency** the Main Settings section. For details, see "URL Sequence Monitor Settings" on page 881.
3. Configure the individual steps for the URL sequence. You do this by using the **Add Step** button in the Main Settings section. For more information, see "Creating a URL Sequence" on page 578.
4. Configure the Advanced Settings as necessary. For details, see "URL Sequence Monitor Settings" on page 881.
5. Configure the Threshold Settings for the monitor. The thresholds can be set for individual steps or for the whole monitor. For details, see "URL Sequence Monitor Settings" on page 881.
6. Click **OK** to create the new monitor instance.

   Once you have added a URL Sequence Monitor, you can edit the monitor configuration settings using the same steps as with other monitors.

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 that you either:

- Import the server certificate as described below.
- Select the **Accept Untrusted Certs for HTTPS** option in the Advanced Settings as described in "URL Sequence Monitor Settings" on page 881.

To import a server certificate:

1. Check the certificates already in the keyStore, from the <**SiteScope root directory**>/**SiteScope/java/lib/security** directory, by entering:

   ```
   ../../bin/keytool -list -keystore cacerts
   ```

2. Import the certificate, from the <**SiteScope root directory**>/**SiteScope/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 **jssecacerts** file.

3. Make a copy of <**SiteScope root directory**>/**SiteScope/java/lib/security/cacerts** and rename it <**SiteScope root directory**>/**SiteScope/java/lib/security/jssecacerts**. After doing this, manually check to make sure the file **jssecacerts** is located in the <**SiteScope root directory**>/**SiteScope/java/lib/security** directory. The reason for creating the **jssecacerts** file is that the default **cacerts** file is overwritten every time SiteScope is upgraded or re-installed. Creating a copy with a different name allows new certificates to be imported and not be overwritten with future installations or upgrades.

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, 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.

Some Web sites use dynamically generated link references on pages generated by server-side programming. While these Web pages do not contain client-side programs, frequently changing link references or cookie data can make it difficult to set up and maintain a URL Sequence Monitor.

Dynamic Content Workarounds

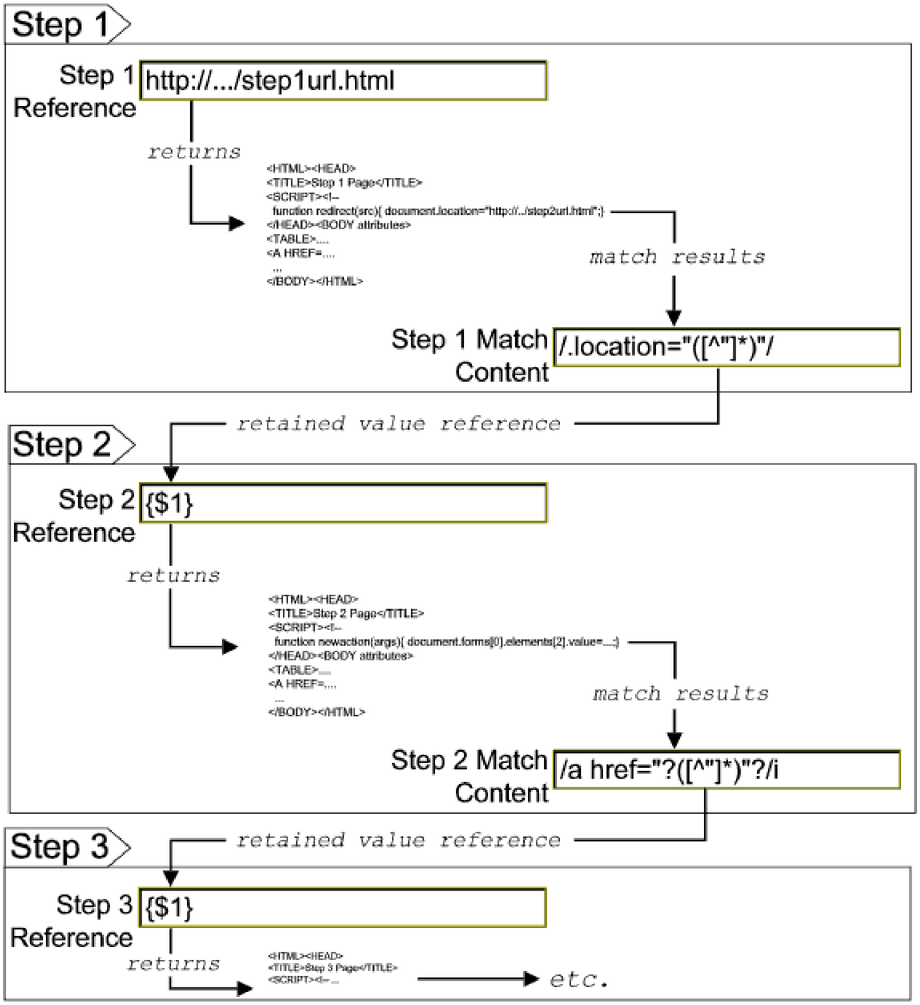
There are several ways to make a SiteScope URL Sequence monitor perform actions controlled by client-side programs and other dynamic content. Several of these workarounds are presented below. The workarounds generally require knowledge of the principles of Web page construction, CGI programming, Perl-style regular expressions, and the programming used to support the Web site being monitored.

Dynamic Content	SiteScope Workaround
A Web page contains a script which controls a link to another URL. **Example:** onClick = "document.location='http://...	Use a Match Content regular expression in the sequence step for the subject page to retain the **filename.ext** value from the .location="filename.ext" match pattern. The retained value can then be passed as a URL in the **URL** 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 **POST Data** box in the URL Sequence step dialog page. 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 <A HREF=...> links.	Use a Match Content regular expression to return the filename.ext value from the HREF="filename.ext" pattern and pass it to the **URL** box of the next sequence step.
A client-side program generates HTML content which, after interpretation by a Web browser, includes forms submitted to a CGI program.	Manually enter the NAME=VALUE pairs for the subject sequence step. This is done in the **POST Data** box in the URL Sequence step dialog page. This requires familiarity with the script, the form structure, and CGI request headers.

Dynamic Content	**SiteScope Workaround**
A script dynamically sets the ACTION attribute of an HTML <FORM> tag.	Manually enter the ACTION URL for the next sequence step. This is done in the **URL** box under **Reference Type** in the URL Sequence step dialog page. This requires familiarity with the script.
A script dynamically sets the METHOD attribute of an HTML <FORM> tag.	Manually enter the POST or GET data for the next sequence step. For POST methods, enter the data in the **POST Data** box in the URL Sequence step dialog page. For GET methods, enter the ACTION URL plus the &NAME=VALUE pairs in the **URL** box under **Reference Type** in the URL Sequence step dialog page. 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 expressions 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 only uses one set of parentheses and thus references the retained value as {$1}.



```
<HTML><HEAD>
<TITLE>Step 1 Page</TITLE>
<SCRIPT><!--
 function redirect(src){ document.location="http://../step2url.html";}
</HEAD><BODY attributes>
<TABLE>....
<A HREF=....
 ...
</BODY></HTML>
```

```
<HTML><HEAD>
<TITLE>Step 2 Page</TITLE>
<SCRIPT><!--
 function newaction(args){ document.forms[0].elements[2].value=...;}
</HEAD><BODY attributes>
<TABLE>....
<A HREF=....
 ...
</BODY></HTML>
```

```
<HTML><HEAD>
<TITLE>Step 3 Page</TITLE>
<SCRIPT><!-- ...
```

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 via 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.

For details on the steps and settings you use to create a URL sequence, see "URL Sequence Steps Settings" on page 887.

Configuring This Monitor

For details on configuring this monitor, see "URL Sequence Monitor Settings" on page 881.

Creating a URL Sequence

The core of the URL Sequence Monitor is the sequence of URL and associated action requests that are performed by the monitor. The following sections describe the steps and settings you use to create an URL sequence.

Starting a New URL Sequence

The URL sequence must begin with an initial URL. You configure the first URL in the sequence in the URL Sequence panel.

To start a new URL Sequence:

1. In the Main Settings panel of the New URL Sequence Monitor properties tab, click the **Add Step** button. The URL Sequence step dialog box opens.
2. Enter the initial URL address in **Reference Type** field. 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.

3 Complete the other settings as necessary. Generally, the URL is sufficient for the first step of most URL sequences. See the section “URL Sequence Steps Settings” for more information.

4 Click the **Ok** button at the bottom of the dialog box to add the step.

SiteScope makes a request for the URL entered for the **Reference Type** URL. 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.

Defining Additional Sequence Steps

When you have entered the first step, you are ready to 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:

- Go to URL Manually
- Following a Hyperlink
- Selecting a Form Button
- Selecting a Frame Within a Frameset
- Following a META REFRESH Redirection

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.

Tools for Viewing Sequence Steps and Content

The buttons at the bottom of the step dialog page provide you with some additional tools useful for working with URL sequences. Next to the **OK** and **Cancel** buttons are two buttons you use as described below:

- **Show Source**. Click this button 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.
- **Show Page**. Click this button to open a new browser window that displays the URL in a regular browser view. You can use this window to match the **Link** and **Form** data displayed in the URL Sequence Monitor step dialog form with the elements as displayed on the Web page.

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 allows 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.

Complete the following steps if you want to direct SiteScope to go to a URL other than those listed in the Links list.

To request a specific URL manually:

1. For the **Reference Type** option, click the radio button to the left of the **URL** text entry box.
2. Type the URL you want SiteScope to go to in the URL text entry box.
3. Complete the other step settings as necessary. Include any CGI Post or Get data that may be required. For more information, see “URL Sequence Steps Settings” on page 887.

4 Click the **Ok** button to add the step.

5 Use the steps in this section to add additional sequence steps. After you have added all the steps to the URL sequence, click the **OK** button at the bottom of the monitor Properties tab to add the monitor to SiteScope.

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 **Link** radio button. Use the following steps to add a link step to the sequence.

To request a URL by following a hyperlink

1 For the **Reference Type** option, click the radio button to the left of the **Link** item.

2 Click to expand the drop-down menu 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.

3 Complete the other step settings as necessary. For more information, see "URL Sequence Steps Settings" on page 887.

4 Click the **Ok** button to add the step.

5 Use the steps in this section to add additional sequence steps. After you have added all the steps to the URL sequence, you must click the **OK** button at the bottom of the monitor Properties tab to add the monitor to SiteScope.

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

For example, the Search button on a company's search page might be listed as:{[1]http://www.CompanyName.com/bin/search}search

To submit Form data or request:

1 For the **Reference Type** option, click the radio selection button to the left of the **Form** item. The drop-down list to the right of the **Form** item lists the form Submit buttons found on the current page.

2 Click to expand the drop-down menu 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 the note below about client-side programs.

3 Below the list of form submit buttons is the **POST Data** field that contains a listing of form input items available for this page. Locate those that pertain to the form associated with the submit button you selected and type the appropriate data in to the **POST Data** text box. Note that there may be more than one form on the page.

Post Data is submitted as name-value pairs. Enter the data you want to submit after the equals sign (=) corresponding to the Name parameter for that data. You may need to view the form in a separate browser window to determine the format and expected values for the **POST Data** values.

4 Complete the other step settings as necessary. For more information, see “URL Sequence Steps Settings” on page 887.

5 Click the **OK** button to add the step.

6 Use the steps in this section to add additional sequence steps. After you have added all the steps to the URL sequence, you must click the **OK** button at the bottom of the monitor Properties tab to add the monitor to SiteScope.

Selecting a Frame Within a Frameset

Complete the following steps 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.

To select an HTML page that is part of a Frameset:

1. Click the radio button to the left of the Frame text entry box.
2. 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.
3. Complete the other step settings as necessary. For more information, see “URL Sequence Steps Settings” on page 887.
4. Click the **Ok** button to add the step.
5. Use the steps in this section to add additional sequence steps. After you have added all the steps to the URL sequence, you must click the **OK** button at the bottom of the monitor Properties tab to add the monitor to SiteScope.

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.

To follow a META Refresh redirection:

1. Click the radio button to the left of the Refresh text entry box.
2. Click the arrow on the right of the box to display all available Refresh filenames. Normally there is only one filename. Select the file that you want SiteScope to retrieve.
3. Complete the other step settings as necessary. For more information, see “URL Sequence Steps Settings” on page 887.

4. Click the **Ok** button to add the step.
5. Use the steps in this section to add additional sequence steps. After you have added all the steps to the URL sequence, you must click the **OK** button at the bottom of the monitor Properties tab to add the monitor to SiteScope.

Editing URL Sequence Steps

You can edit the steps in a URL sequence once 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. use the following steps to edit a step in a URL Sequence.

Note: Editing any step of a URL sequence may impact 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.

To edit a sequence step:

1. In the properties tab for the subject URL Sequence Monitor, click to edit the monitor instance.
2. In the Main Settings section, click the ✎ button to the right of the step you want to edit. The sequence page for that step opens.
3. Edit the settings for the step as necessary.
4. Click the **OK** button at the bottom of the step page to update the step settings. The sequence page closes. The properties view for the monitor is updated with the revised step settings.
5. Click the **OK** button at the bottom of the monitor Properties tab to update the monitor. SiteScope attempts to execute the changes to the step. The results of the monitor run are displayed in SiteScope Dashboard.

Deleting URL Sequence Steps

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 since, in most cases, one step is dependent on data returned by the previous step. Use the following steps to delete URL sequence steps:

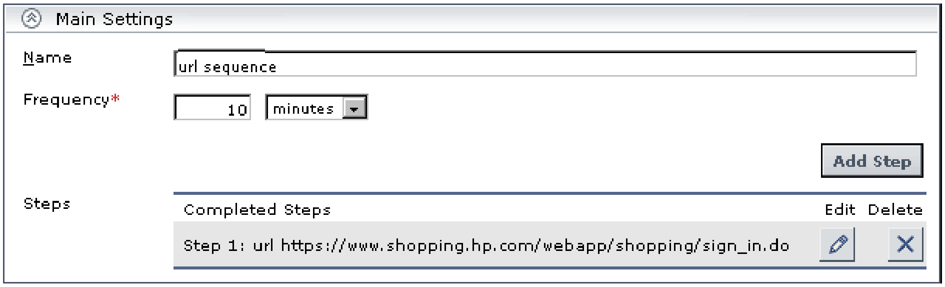
To delete sequence steps:

1. In the properties tab for the subject URL Sequence Monitor, click to edit the monitor instance.
2. In the Main Settings section, click the ☒ button to the right of the step you want to delete.
3. Click the **OK** button at the bottom of the step page to update the step settings. The sequence page closes. The properties view for the monitor is updated with the revised step settings.
4. Click the **OK** button at the bottom of the monitor Properties tab to update the monitor. SiteScope attempts to execute the changes to the step. The results of the monitor run are displayed in SiteScope Dashboard.

Entering an Encrypted or Unencrypted Password

To enter an encrypted or unencrypted password:

1. Right-click the URL Sequence monitor whose password you want to set. Select **Edit**. The URL Sequence page opens.



Main Settings

Name: url sequence

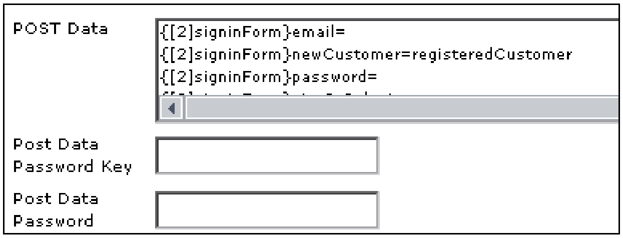
Frequency*: 10 minutes

Steps

Completed Steps	Edit	Delete
Step 1: url https://www.shopping.hp.com/webapp/shopping/sign_in.do		☒

2. In the Main Settings section, click **Add Step**. The URL Sequence dialog box opens.

3 Scroll down to **POST Data.** Information supplied by the URL site is displayed. In this example, no password has been assigned to the URL Sequence monitor. The **password=** field is empty:



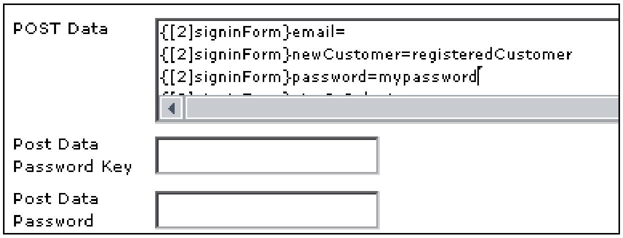
POST Data

```
{[2]signinForm}email=
{[2]signinForm}newCustomer=registeredCustomer
{[2]signinForm}password=
```

Post Data Password Key

Post Data Password

4 To give an unencrypted password to the URL monitor, enter the password in the **password=** field in the **POST Data** text box. The password you enter is displayed in the text box.



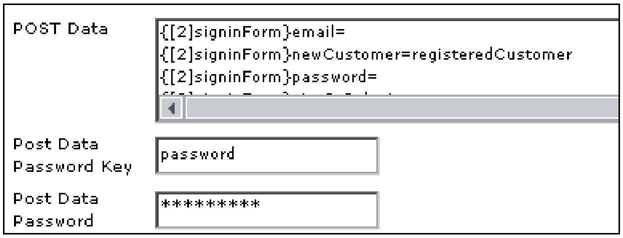
POST Data

```
{[2]signinForm}email=
{[2]signinForm}newCustomer=registeredCustomer
{[2]signinForm}password=mypassword
```

Post Data Password Key

Post Data Password

To give an encrypted password to the URL monitor form, enter 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:



POST Data

```
{[2]signinForm}email=
{[2]signinForm}newCustomer=registeredCustomer
{[2]signinForm}password=
```

Post Data Password Key: password

Post Data Password: *********

5 Click **OK** to save your settings and close the URL Sequence dialog box. Click **Cancel** to exit without saving your settings.

Retaining and Passing Values Between Sequence Steps

One important feature of the Match Content capability in URL Sequence Monitor is the ability to match, retain, and then reference values from one URL sequence step for use as input in a subsequent step. Using one or more sets of parentheses as part of a Match Content regular expression instructs SiteScope to remember the values matched by the pattern inside the parentheses. These values can then be referenced using the syntax described in the following example.

Example

Suppose you create a URL Sequence Monitor and include a Match Content expression for the first step to capture some session information. The Step 1 Match Content expression could be in the form of

```
/[\w\s]*?(pattern1)[\/\-\=]*?(pattern2)/
```

The two sets of parentheses in this expression instruct SiteScope to retain the two values matched by pattern1 and pattern2. To use these values as input to the **next** step in the URL sequence, use the syntax {**$valuenum**}. In this example, the string {$1} references the value matched by pattern1 and {$2} references the value matched by pattern2.Use the above syntax for passing the referenced values to the URL sequence step immediately following the step in which the content match was made (step 1 to step 2 in our example). You can retain and pass matched values from one step to any other subsequent step by using a compound syntax of {**$$stepnum.valuenum**}. If, in our example, you want to use the value matched by pattern1 in step 1 as input in a FORM or URL request in step 4 of the URL sequence, you would include the syntax {$$1.1} in Step 4. To reference the value matched by pattern2, use the {$$1.2} syntax.

Sharing Cookies Between Monitor Runs and Configured Monitors

The URL Sequence Monitor also supports sharing cookies between monitor runs and between configured monitors. This is done by maintaining a persistency of both session cookies and permanent cookies that can be queried, updated and shared among other URL Sequence monitors.

Suppose you have a number of different URL Sequence Monitors that are currently configured on a SiteScope server. Assume that all the monitors simulate a URL transaction in which at least one of the steps uses a session cookie to send to the server instead of logging in each time. Using Cookie Persistency, you can configure one monitor to save the cookies it receives and configure all the other monitors to load the cookies. This can save system costs if there is a charge for each request to the login server from the monitoring tool. The monitor can 'log in' once and reuse the credentials from the login by other monitor runs and monitor instances. Thus, only one monitor needs to contain a login step. All the others can skip this step and send the login credentials in a cookie instead.

Notes:

- Configure the monitor designated to save cookies to run at a frequency that is not less than the time frame of the session to ensure 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 ensure 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 ensure that the monitor saving cookies runs first.

Configuring This Monitor

For details on configuring this monitor, see "URL Sequence Monitor Settings" on page 881.

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.

The Web Script Monitor runs the scripts created in the HP Virtual User Generator (VuGen). You use VuGen to create a script that emulates end-user actions. You can create the script with the steps that you want monitored on target Web sites.

Note: The Web Script Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information.

Note to HP Business Availability Center users: The Web Script Monitor is not available when working in HP Business Availability Center. The monitor's data cannot be reported to HP Business Availability Center.

What to Monitor

You can create transactions to monitor pages that are critical to your Web applications, pages that are generated dynamically, and pages that depend upon other applications to work correctly (such as pages that utilize a back-end database).

Counter Measurements and Transaction Breakdown Data

Each time the Web Script Monitor runs the VuGen script, it returns the transaction breakdown and performance data. The VuGen script also includes content match functionality, enabling you to check images, texts, links, and other areas of the Web site.

In addition, the monitor's reported data can include the following measurements:

- The amount of time needed to establish an initial connection with the Web server performing the transaction.
- The amount of time taken to establish an SSL connection for HTTPS connections.
- The time in milliseconds for the transaction to be run.
- Whether the transaction passed or failed to connect and perform its required steps.
- Number of pages accessed when running the transaction.
- Number of errors that occurred during the transaction run.

The monitor can provide early indicators of the following performance issues:

- Excessive connection or retry times.
- Slow DNS resolution or other problems with the DNS server.
- Problems along the network or whether the server is responsive to requests.
- Delays or failures in secured or authorized connections.
- Overall network quality.
- Web server delays.

Each of the measurements is available as a parameter for assigning thresholds. This means that thresholds can be set for specific transactions and measurements, providing status indicators per transaction.

For details on selecting measurement counters, see “Selecting Counters” on page 596.

Setting up the Web Script Monitor

Prior to configuring the Web Script Monitor in SiteScope, you must create the script in VuGen. The monitor runs only those scripts created in VuGen.Here is an overview of the steps necessary to set up the Web Script Monitor.

1 **Download HP Virtual User Generator.**

Go to the HP Downloads site (http://downloads.mercury.com) and download the HP Virtual User Generator from the download options under SiteScope. The download is available directly from the SiteScope downloads page.

To enable monitoring, you must also download the latest HP Virtual User Generator Feature Pack.

2 **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 is easy-to-use and contains different access points to obtaining help. For details, see "Getting Started" on page 592.

3 **Use the supported protocols in Virtual User Generator to create your script.**

It is recommended to use the Web (Click and Script) protocol to create your script for use in SiteScope. For a list of all the supported protocols and for details on the Web (Click and Script) protocol, see "Supported VuGen Protocols" on page 593.

4 **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.

Checkpoints are recommended for checking content while running the VuGen script.

For details, see "Inserting Transactions and Creating Checkpoints" on page 594.

5 **Save the script's runtime files into a zip file and save the zip file into the appropriate directory.**

For details, see "Saving and Storing the Script" on page 595.

6 Ensure that the script runs properly in VuGen before continuing.

For details, refer to "Working with VuGen" > "Running Vuser Scripts in Standalone Mode" in the VuGen guide.

7 Create the Web Script Monitor in SiteScope.

For details, see "Web Transaction Monitors User Interface Settings" on page 851.

Working with VuGen

VuGen can be used to automatically generate 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.

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 feature.
- 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 on the workflow, refer to "Working with VuGen" > "Viewing the VuGen Workflow" in the VuGen guide.

For more detailed information on creating scripts, refer to "Working with VuGen" > "Recording with VuGen" > "Creating New Virtual User Scripts" in the VuGen guide.

Supported VuGen Protocols

The following are the protocols supported for the Web Script Monitor.

Web (Click and Script) Protocol

This is the recommended protocol to use to record scripts to be run by the Web Script Monitor.

Web (Click and Script) is a new approach to Web scripting. It introduces a GUI-level scripting API, and a quicker way to generate scripts.

- Easy-to-use scripting.
- Intuitive API functions describe user actions on Web objects (button, text link etc.).
- In tree view, the steps are grouped according to their pages.
- In snapshot viewer, the object corresponding to the active step is highlighted.

For details on using this protocol, refer to the “Creating Web Vuser Scripts” and “Working with Web (Click and Script) Vuser Scripts” sections under “E-Business Protocols” in the VuGen guide.

Web (Click and Script) Limitations

- Records and emulates on Internet Explorer version 6 only.
- Does not support recording on Windows 2003.
- Does not support VBScript and applets.
- Does not support user actions on ActiveX objects and Macromedia Flash.
- Supports only English language applications.

Note: If any of these limitations affect your ability to record a script, use VuGen’s Web (HTTP/HTML) Protocol instead. For details, see below. For more information on choosing a protocol, refer to “E-Business Protocols” > “Choosing a Web Vuser Type” in the VuGen guide.

Web (HTTP/HTML) Protocol

This is the standard VuGen protocol for recording Web applications.

When recording a Web (HTTP/HTML) script, VuGen records the HTTP traffic and server response over the Internet. The scripts contain detailed information about your actions in the browser.

The Web (HTTP/HTML) Vuser provides two recording levels: HTML-based script and URL-based script. These levels let you specify what information to record and which functions to use when generating a Vuser script.

For details on using this protocol, refer to the "E-Business Protocols" > "Creating Web Vuser Scripts" in the VuGen guide.

Inserting Transactions and Creating Checkpoints

- ➤ While creating your VuGen script, you must insert transactions into the script. These transactions provide the breakdown performance data reported by the monitor.

  For details on transactions, refer to "Working with VuGen" > "Enhancing Vuser Scripts" > "Inserting Transactions into a Vuser Script" in the VuGen guide.

- ➤ VuGen's Content Check mechanism allows you to check the contents of a page for a specific string. This is useful for detecting non-standard errors. It is recommended that you include content check checkpoints in your script.

  For details on checkpoints, refer to the "Checking Web Page Content" and "Verifying Web Pages under Load" sections under "E-Business Protocols" in the VuGen guide.

Saving and Storing the Script

The script you create in VuGen must be saved as a zip file. It is recommended to save only the runtime files. For details, refer to the "Recording with VuGen" and "Using Zip Files" sections of the VuGen guide.

When saving the zip file:

- ensure that the zip file has the same name as the script
- ensure 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 dropdown list of available scripts under Main Settings 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** field in General Preferences. The scripts stored in the location you enter appear in the dropdown list of available scripts under Main Settings 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.

Selecting Counters

You use the features associated with the **Counters** setting to choose and manage the metrics you want to monitor with the Web Script Monitor. Use the following steps to select and add counters.

To select or add counters:

1. When adding or editing a monitor, in the Main Settings area, click **Get Counters** to access the script transactions. The Get Counters selection dialog box opens.
2. Use the features in the Get Counters selection dialog box to select the counters you want to monitor. The first list of counters applies to all the transactions in the script and is called **Total**. The **Status** counter is the only counter that is in the **Total** 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.

   Note: Not all counters return values for all transactions.

3. Use the check boxes to select the counters to be monitored. There is no limit to the number of counters that can be monitored.
4. Click **OK** to add the selected counters to the monitor configuration. The Get Counters selection dialog box closes and the monitor properties are updated with your selection.

Use the following steps to remove a counter from the selected counters list.

To remove or edit counters:

1. Click to edit the monitor for which you want to remove counters. Alternately, you may select the monitor you want to edit and click the Properties tab and click the **Edit** button. The monitor Properties tab opens.
2. Click the **Get Counters** button to open the Get Counters selection dialog box.

3 Clear the check box to the left of the current counter you want to remove.

At this point, you may add other counters to the monitor by clicking the applicable check boxes.

4 Click **OK** at the bottom of the monitor Properties tab to update the monitor.

The following table lists all the counter metrics available for the monitor. Not all the counters report on all the transactions.

Name	Description
Retry Time	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.
DNS Time	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.
Connection Time	Displays the amount of time needed to establish an initial connection with the Web server performing the transaction. The connection measurement is a good indicator of problems along the network or whether the server is responsive to requests.
SSL Handshaking Time	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. The SSL handshaking measurement is only applicable for HTTPS communications.
Network Time to First Buffer	Displays the amount of time that passes from the moment the first HTTP request is sent until receipt of ACK. The network measurement is a good indicator of network quality (look at the time/size ratio to calculate download rate).

Name	Description
Server Time to First Buffer	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. **Note:** 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.
Download Time	Displays the time from the receipt of the first buffer until the last byte arrives. Download time is a combination of server and network time, since 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. 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.
Client Time	Displays the time during the script run when the client is not sending or receiving data from the server.
Duration	The time in milliseconds for the transaction to be run.
Status	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.
Size	The size in bytes received from the Web sites being monitored by the transaction.
Number of Errors	Number of errors that occurred during the transaction run.
Number of Pages	Number of pages accessed when running the transaction.

Advanced Information and Troubleshooting

The Web Script Monitor uses an internal engine to run the VuGen scripts you create. This section includes some advanced issues and troubleshooting.

SiteScope makes a copy of the script created in VuGen and stores it in a location within the SiteScope directory. SiteScope makes the necessary modifications for the script to be run properly by the Web Script Monitor. These modifications are automatic and cannot be manually duplicated. They include:

- Disabling the **Download Snapshots** operation.
- Disabling the **Think Time** operation.
- Disabling the **Iterations** operation.

Therefore:

- If there is any change made to the script in VuGen, including the name of the script, and you want the Web Script Monitor to run the revised version of the script, you must edit the monitor in SiteScope and select the edited script in its saved location.
- Each script must have a unique name even if the different zip files for the scripts reside in different directories.
- The name of the zip file selected for the monitor must be the same as the name of the script created in VuGen.

Troubleshooting

- Each time the monitor is run, a log is created. You can view the log to troubleshoot the monitor if you see there is a problem running the scripts. The logs are stored in **<SiteScope root directory>/cache/temp/WebScript/<name of script>/log**. You can search for the appropriate log based on the name of the script run by the monitor and the time the log was created.

  This directory is cleaned out every time SiteScope is restarted, which is every 24 hours by default.
- If the log files do not give you the necessary information to determine why the script is not running properly, run the script in VuGen. For details, refer to “Running Vuser Scripts in Standalone Mode” in the VuGen guide.

- If all the transaction breakdown counters for the monitor are reporting a status of -1 and there is a reported time for the Duration counter (the total running time of the transaction), it could be because the transaction breakdown times exceed the total running time. This can occur in rare cases because of the way the transaction breakdown times are calculated and because the Duration is an actual measurement of the total transaction time from start to finish, with no additional calculations. If the problem persists for a specific transaction, it is recommended that you adjust the counters selected for the transaction.

Configuring This Monitor

For details on configuring this monitor, see "Web Script Monitor Settings" on page 893.

32

Common Monitor Settings

The following monitor settings tabs contain the common GUI elements on the New Monitor page. For details of other monitor elements not listed here, see the user interface page for the specific SiteScope monitor.

Main Settings

GUI Element	Description
Name	Enter a name that describes the element or system being monitored. Use a useful naming convention for all monitors to make creating view filters and category assignments more effective. **Example:** <hostname:resource_type> or <business_unit resource_name monitored_element> **Default:** SiteScope creates a default name based on the host, system, and/or URL being monitored or the default name defined for the monitor type.
Frequency	Set how often SiteScope attempts to execute the action defined for the monitor instance. Each monitor run updates the status of the monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days. **Default:** Monitor runs once every 10 minutes. **Minimum value:** 15 seconds

Advanced Settings

GUI Element	Description
Show Run Results on Update	Whenever a change is made to a monitor's configuration settings, the monitor is run. Select this option to display the results of that monitor run in a popup dialog box. **Note:** The updated run results are always displayed in the applicable dashboard views for the monitor.
Verify Error	Select to automatically run the monitor again if it detects an error. **Note:** It is recommended not to use this option in large monitoring environments. Significant monitoring delays may result if multiple monitors are rescheduled to verify errors at the same time. The status returned by the Verify Error run of the monitor replaces the status of the originally scheduled run that detected an error. The data from the verify run may be different than the initial error status, causing the loss of important performance data.
Error Frequency	Set a new monitoring interval for monitors that have reported an error condition. **Example:** You may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected. When the monitor's status is no longer in error, the monitor reverts to the run interval specified in the **Frequency** setting. **Note:** Increasing the run frequency of a monitor affects the number of alerts generated by the monitor.
Monitor Schedule	Select a schedule if you want the monitor to run only on certain days or on a fixed schedule. The schedules created in **Preferences** appear in the drop-down list. For more information about creating monitor schedules, see "Range Schedule Preferences Overview" on page 212. **Default:** Monitor is run every day of the week.

GUI Element	Description
Depends On	Select to make the running of this monitor dependent on the status of another monitor. In the representation of the monitor tree, expand the group node and select the check box next to the monitor to which to you want to create dependence. To remove dependence on a monitor, clear the appropriate check box. Use this option to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system. **Example:** Create a system monitor to check the basic availability of a system and then create other monitors that perform more detailed tests of that system. Set the detailed test monitors to be dependent on the status of the monitor checking basic availability. If the system monitor detects that the target system has become unavailable, the dependency relationship automatically disables the other monitors. This also disables any alerts that would have been generated by the dependent monitors. **Default**: No dependency is set for a monitor instance.

GUI Element	Description
Depends Condition	If you make this monitor dependent on the status of another monitor (by using the **Depends On** setting), use this option to select the status condition of the **Depends On** monitor for the current monitor to run normally. The status categories include: ➤ **Good** ➤ **Error** ➤ **Available** ➤ **Unavailable** The monitor being configured is run normally as long as the monitor selected in the **Depends On** field reports the condition selected in this field. **Example:** Select **Good** and this monitor is enabled only when the monitor selected in the **Depends On** field reports a status of **Good**. The current monitor is automatically disabled if the monitor selected in the **Depends On** field reports a category or condition other than **Good**. You can also enable dependent monitors specifically for when a monitor detects an error.
Monitor Description	Enter additional information to describe a monitor. The **Monitor Description** can include HTML tags such as the <BR>, <HR>, and <B> tags to control display format and style. The description text appears on the **Content** tab for the group to which the monitor belongs and in the Dashboard if the **Description** parameter is a selected column.
Report Description	Enter an optional description for this monitor to make it easier to understand what the monitor does. This description is displayed on each bar chart and graph in Management Reports. **Example:** Network traffic or main server response time.

Enable/Disable Monitor Settings

GUI Element	Description
Enable Monitor	If the monitor has previously been disabled, select to enable the monitor. **Default:** Selected
Disable Monitor Indefinitely	When a monitor has been disabled, SiteScope continues to schedule the monitor to run based on the **Frequency** setting for the monitor but the monitor action is not executed. SiteScope records a monitor data log entry for the monitor when it was scheduled to be run but reports the monitor status as disabled in the place of measurement data.
Disable Monitor for the Next Time Period	Enter a time period that the monitor should remain disabled. Select seconds, minutes, hours, or days to define the disable time period as applicable.
Disable Monitor on a One Time Schedule	Use this option to temporarily disable the monitor for a time period in the future. The time period can span more than one day. Enter the start time and end time for the disable period using the format hh:mm. Enter the start and end dates for the disable period using the mm/dd/yy format.
Disable Description	Enter optional descriptive text. This description appears as part of the monitor status in the monitor group display. The disable status text also includes a string indicating which disable option is in force for the monitor, for example Disabled manually indicates that the monitor was disabled using the **Disable Monitor Indefinitely** option.

Enable/Disable Alert Settings

GUI Element	Description
Disable Alerts with respect to this monitor	Displays all the alerts, within a monitor tree hierarchy, that are associated with the current monitor instance, including alerts added to the monitor's parent group or to the SiteScope. If no alerts have been configured for this monitor instance, the monitor's parent group, or globally for the SiteScope, a message appears instead of the alert list.
Enable All Associated Alerts	If the alerts associated with this monitor have previously been disabled, select to enable the alerts. **Default:** Selected
Disable All Associated Alerts for the Next Time Period	Enter a time period that the associated alerts should remain disabled. Select seconds, minutes, hours, or days to define the disable time period as applicable.
Disable All Associated Alerts on a One Time Schedule	Use this option to temporarily disable the associated alerts for a time period in the future. The time period can span more than one day. Enter the start time and end time for the disable period using the format hh:mm. Enter the start and end dates for the disable period using the mm/dd/yy format.
Disable Description	Enter optional descriptive text.

Threshold Settings

Description	Use to set conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. You can also set monitor thresholds using a baseline. Status threshold criteria for each monitor instance can be set for the following status conditions: ➤ **Error if** ➤ **Warning if** ➤ **Good if**
Important Information	You can apply multiple status threshold criteria for each status condition per monitor instance. A single monitor instance may have one or more criteria used to determine **Error** status, one or more conditions to determine **Warning** status, and one or more conditions to indicate **Good** status. Most monitor types include one default setting for each of the three status conditions.
Useful Links	"Setting Status Thresholds" on page 396 "Setting Monitor Thresholds Using a Baseline" on page 398

The following elements are found in the Threshold Settings area:

GUI Element	Description
If Unavailable	Select a status assignment for when the monitor is not available from the following options: ➤ **Set Monitor Status According to Thresholds.** The monitor gets a new status according to the thresholds. ➤ **Set Monitor Status to Good.** The monitor's status is set to Good when it is unavailable without thresholds being checked. ➤ **Set Monitor Status to Warning.** The monitor's status is set to Warning when it is unavailable without thresholds being checked. ➤ **Set Monitor Status to Error.** The monitor's status is set to Error when it is unavailable without thresholds being checked. **Note:** A monitor instance can have a status of Unavailable as well as a status of Good, Warning, or Error. Alerts are triggered according to availability, status, or both availability and status, depending on how the alert is configured. For details, see "Understanding Alerts" on page 1184.
Default Status	The status of the monitor (Good, Warning, or Error) if the threshold criteria for the monitor instance are not met. **Default:** Good
Baseline Status	Indicates whether the monitor has baselining enabled. If enabled, baseline status contains baseline type (static, rolling) and calculated baseline. For details, see "Setting Monitor Thresholds Using a Baseline" on page 398.

GUI Element	Description
Baseline	Button appears only when editing a monitor. Click to open the Enable Baseline dialog box. In the Enable Baseline dialog box, enter the baseline data interval for gathering statistics for computing a static baseline. The baseline interval is based on the specified number of days starting from the current day. The baseline interval must be a positive integer. **Note:** The baseline becomes active only after the monitor has accumulated data for the specified baseline interval.
Error if	Set the conditions for the monitor instance to report an **Error** status.
<**measurement** >	Select the measurement parameter from the drop-down list to determine the status of this monitor instance. The list of measurements is dynamically updated based on the type of monitor you are configuring. **Default:** Default measurements exist for many monitor types and differ per monitor type. For many default measurements, there are corresponding defaults for the operator and value fields.
<**operator**>	Select an operator for the measurement from the drop-down list. The corresponding value is entered in the next field. ➤ >= Greater than or equal to ➤ > Greater than ➤ == Equals ➤ **!**= Not the same as ➤ <= Less than or equal to ➤ < Less than ➤ **contains** Contains the value entered ➤ **!contains** Does not contain the value entered
<**measurement value**>	Enter a value applicable to the measurement parameter in the field following the operator selected.

GUI Element	Description
New Error if	Click this button to configure additional thresholds that determine **Error** status. For each threshold, select the measurement and operator, and enter a value for the measurement. By default, two thresholds are displayed when you first configure the monitor.
Warning if	Set the conditions for the monitor instance to report a **Warning** status. For each threshold, select the measurement and operator, and enter a value for the measurement.
New Warning if	Click this button to configure additional thresholds that determine **Warning** status. By default, only one threshold is displayed when you first configure the monitor.
Good if	Set the conditions for the monitor instance to report a **Good** status. For each threshold, select the measurement and operator, and enter a value for the measurement.
New Good if	Click this button to configure an additional threshold that determines **Good** status. By default, only one threshold is displayed when you first configure the monitor.

Link Monitor to CI

GUI Element	Description
Select CIs button	You can link between this monitor instance and any existing, logical configuration item (CI) in HP Business Availability Center's Universal configuration management history database. This link or relationship enables the monitor to pass KPI status to the CI to which it is linked. This is in addition to the monitor's corresponding CI that is created automatically when the monitor instance is created. The Select CIs button opens the dialog box in which you select an existing CI from a CMDB view to link to this monitor instance. For details on selecting and working with views, see "View Explorer" in *Reference Information*. **Note:** The Link Monitor to CI Settings are available only when adding a SiteScope monitor and cannot be set while editing a monitor.

Custom Properties

GUI Element	Description
<custom property>	This area lists those custom properties that have been created for this SiteScope. If no custom properties have been created, this section appears but is empty. If custom properties have been created, they are listed here and you configure as needed. For details on creating custom properties, see "Creating Custom Properties" on page 1367.

HP BAC Logging

Description	Use the HP BAC Logging settings area to control what data a monitor forwards to the HP Business Availability Center database.
Important Information	Your selection should be based on how much data is relevant to report to BAC for this monitor and how much space the BAC database has for this data.

The following elements are found in the Logging to Business Availability Center area:

GUI Element	Description
Do not report to HP Business Availability Center	Select when you do not want any of the measurements for this monitor to be transferred to HP Business Availability Center.
Report everything (all monitors and all measurements)	Select to send all monitor data to HP Business Availability Center for each time that the monitor runs. This option enables the largest data transfer load.
Report monitor level data (no measurements)	Select this option to send only monitor category (error, warning, good), status string, and other basic data for each time that the monitor runs. No information on specific performance counters is included.
Report monitor level data and measurements with thresholds	Select to send monitor category (error, warning, good), status string, as well as performance counter data for only those measurement counters that have thresholds configured thresholds (for example, Error If, Warning If, etc.). The data is sent for each time that the monitor is run.
Report status changes (no measurements)	Select to send only monitor category (error, warning, good), status string, and other basic data only when the monitor reports a change in status. No information on specific performance counters is included. This option enables the smallest data transfer load.

Category Settings

GUI Element	Description
Assigned categories	The Category settings are used to filter items in the monitor tree. If no categories have been created for the SiteScope, this section appears but is empty. If categories have been created, they are listed here and you configure as needed. For details on creating categories, see "Working with Categories" on page 173.

Note: HTML code entered in monitor text fields is checked for validity and security, and corrective action is taken to fix the code (for example, mismatched tags or code that was truncated because it spanned more than one line). If malicious HTML code or Javascript is detected, the entire field is rejected.

33

SiteScope New Monitor User Interface

This chapter includes the pages and dialog boxes that are part of SiteScope New Monitor.

This chapter describes:	**On page:**
Configuring New SiteScope Monitor	615

Configuring New SiteScope Monitor

Description	Enables you to define a new monitor in a monitor group. **To access:** Right-click a monitor group. Select **New Monitor**. Alternatively, select a monitor group, and click the **Contents** tab in the right pane. Click the **New Monitor** button.
Important Information	Monitors can be created only in a SiteScope group.

The following elements are found in the New Monitor page:

Main Settings

GUI Element	Description
Recently Used Monitors	Select a monitor from a display of monitors that were recently added to the SiteScope Monitor Groups. **Note:** ➤ The five most recently selected monitors are listed here. ➤ The displayed monitors may change as more selections are made.
Monitors List and Category Filter	You select a monitor to deploy by selecting it from the full list of available monitors or by one of the following: ➤ **Monitor:** Enter a monitor name in the **Monitor** field. To search for a monitor name, you can also enter a regular expression. ➤ **Category:** Click the arrow to the right to select a monitor category from the list detailed below. **Note:** Click on the arrow in the header of the **Monitor** column to change the alphabetical order (ascending or descending) of the listed monitors.
Category	You can add a monitor by selecting one of the following categories and clicking on a monitor in that category: ➤ Application Monitors ➤ Database Monitors ➤ Generic Monitors ➤ Integration Monitors ➤ Network Monitors ➤ Server Monitors ➤ Stream Monitors ➤ Web Transaction Monitors

34

SiteScope Group Settings User Interface

This chapter includes the pages and dialog boxes that are part of SiteScope New Group.

This chapter describes:	On page:
SiteScope Group Settings	617

SiteScope Group Settings

Description	Enables you to define a new group for SiteScope, or a subgroup for an existing monitor group. **To access:** Right-click the SiteScope container, or an existing monitor group and select **New Group**.
Useful Links	"Manage SiteScope Monitor Groups" on page 374

The following elements are found throughout the New Group page:

Main Settings

GUI Element	Description
Group Name	Enter text description for the monitor group. Choose a name that describes the content of the group, or the purpose of the monitors added to the group. For example, <hostname> or <business_unitresource_name> or <resource_type>.

Advanced Settings

GUI Element	Description
Group Description	Enter additional information to describe a group.
Depends On	Select a monitor on which the monitor group is depended. This monitor acts as the “heartbeat” monitor and checks the basic availability of the system. If the “heartbeat” monitor detects a problem in the target system, the dependency relationship automatically disables all the monitors in the monitor group. Use this option to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system.
Depends Condition	Select the **Depends Condition** that the **Depends On** monitor should have for the current monitor group to run normally. If the selected condition is not satisfied then the monitor selected in the **Depends On** field is automatically disabled. The conditions are: ➤ Good ➤ Error ➤ Available

Category Settings

GUI Element	Description
Assigned categories	Filters items in the SiteScope views. For more details, see “Views and Categories” on page 171.

35

Application Monitors User Interface Settings

This chapter includes the pages and dialog boxes that enable you to add and edit SiteScope monitors.

Active Directory Replication Monitor Settings

Description	The Active Directory Replication Monitor allows you to monitor the time that it takes replication to occur between up to ten Domain Controllers. The error and warning thresholds for the monitor can be set on each of the monitored Domain Controllers. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	➤ This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ➤ Monitors must be created in a group in the monitor tree.
Useful Links	"Active Directory Replication Monitor Overview" on page 409.

The Add/Edit Active Directory Replication Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Domain Controller	Select the Domain Controller that contains the replicated data.
Replicating Domain Controllers	Enter a comma separated list of Domain Controllers that replicate data from the Domain Controller entered above.

GUI Element	Description
Username	Enter either the user name or the entire Security Principal of a Domain Admin account. If a user name is given, the default security principal is created from the root context of the Domain Controller. For example, if you enter in 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.
Password	Enter the password for the Domain Admin account.

Advanced Settings (Monitor Specific)

GUI Element	Description
Maximum Replication Time	Enter the maximum amount of time for replication to occur. The monitor goes into error if any of the Replicating Domain Controllers exceed this replication time.
Polling Interval	The amount of time this monitor should wait between queries of the Replicating Domain Controllers. A higher number reduces the number of LDAP queries against the servers.
Path to Directory	The path to a Directory in the Active Directory that you want to monitor. This is in the form of an LDAP query. **Default value:** 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.
Trace	This turns on detailed tracing of the LDAP queries being executed. This is used to debug problems.

ASP Server Monitor Settings

Description	Monitor the availability of a Microsoft ASP server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more ASP server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"ASP Server Monitor Overview" on page 410

The Add/Edit ASP Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the ASP Server you want to monitor is running. You cannot directly edit this field. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see "Configure SiteScope to Monitor a Remote Windows Server" on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Apache Server Monitor Settings

Description	Use to monitor the administrative and performance statistics for an Apache server. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Apache Server Monitor Overview" on page 411

The Add/Edit Apache Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.
URL	Choose the server URL you want to verify with this monitor. This should be the Apache server statistics URL which usually has the form of http://<servername>:<port>/server-status?auto.

Advanced Settings (Monitor Specific)

GUI Element	Description
Authorization User Name	If the server you want to monitor requires a name and password for access, enter the name in this box.
Authorization Password	If the server you want to monitor requires a name and password for access, enter the password in this box.
HTTP Proxy	(Optional) A proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, enter the name here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, enter the password here. **Note:** your proxy server must support Proxy-Authenticate for these options to function.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.
Server OS	The operating system that the Apache server is running on. This is used to correctly read server statistics from Apache based on the operating system platform. **Default value:** UNIX

BroadVision Application Server Monitor Settings

Description	Monitor the availability and performance statistics of a BroadVision server. The error and warning thresholds for the monitor can be set on one or more BroadVision server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"BroadVision Application Server Monitor Overview" on page 412

The Add/Edit BroadVision Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Enter the BroadVision root server name of the BroadVision server you want to monitor. For example, 199.123.45.678.
Port	Enter the ORB port number to the BroadVision server you want to monitor. **Example:** 1221
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Check Point Firewall-1 Monitor Settings

Description	Monitor the statistics of a Check Point Firewall-1 server using SNMP. The error and warning thresholds for the monitor can be set on one or more firewall statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Check Point Firewall-1 Monitor Overview" on page 412

The Add/Edit Check Point Firewall-1 Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.
Index	Enter the index of the SNMP object you want to check with this monitor. Non-table object IDs have an index of 0 (zero).

GUI Element	Description
Community	Enter the community name of the Check Point Firewall-1 you want to monitor. You may need to consult with your network administrators about what community names are active in your network environment. **Default value:** public
Host Name	Enter the host name or IP address of the Check Point Firewall-1 server you want to monitor. If the Check Point Firewall is configured to respond to SNMP on a port number other than the default port, enter the port number as part of the server address. **Default value:** 161

Advanced Settings (Monitor Specific)

GUI Element	Description
Retry Delay	The number of seconds that the monitor should wait for a response from the server before retrying the request.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing out. Once this time period passes, the monitor logs an error and reports an error status.

Cisco Works Monitor Settings

Description	Monitor the statistics of a Cisco Works Server using SNMP. The error and warning thresholds for the monitor can be set on one or more Cisco Works server statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Cisco Works Monitor Overview" on page 413

The Add/Edit Cisco Works Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Enter the name of the server you want to monitor.
SNMP Version	Select the version of SNMP to use when connecting.
Community	Enter the community name of the Cisco Works Server you want to monitor (valid only for version 1 or 2 connections). You may need to consult with your network administrators about what community names are active in your network environment. **Default value:** public
SNMP V3 Authentication Type	Select the type of authentication to use for version 3 connections.
SNMP V3 Username	Enter the user name for version 3 connections.
SNMP V3 Authentication Password	Enter the authentication password to use for version 3 connections.

GUI Element	Description
SNMP V3 Privacy Password	Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.
SNMP V3 Context Engine ID	Enter a hexadecimal string representing the Context Engine ID to use for this connection. **Note:** This is applicable for SNMP V3 only.
SNMP V3 Context Name	Enter the Context Name to use for this connection. **Note:** This is applicable for SNMP V3 only.
Timeout	Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.
Retries	Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.
Port	Enter the port to use when requesting data from the SNMP agent. **Default value:** 161
Starting OID	Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered in this field. **Default value:** 1 Edit this field 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 in this field.

GUI Element	Description
MIB File	Select either the Cisco Works MIB file or **All MIBs**. Selecting the Cisco Works MIB file causes only those objects that are described within that MIB file to be displayed. Selecting **All MIBs** causes all objects discovered on the given Cisco Works server to be displayed when browsing counters. If no MIB information is available for an object, it is still displayed, but with no textual name or description.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Counter Calculation Mode	Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are: ➤ a simple delta of the current value from the previous value ➤ a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements **Note:** 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.

Citrix Server Monitor Settings

Description	Monitor the availability of Citrix MetaFrame servers (MetaFrame 1.8 Service Pack 3, MetaFrame XP(s,a,e) Feature Release 1/Service Pack 1, and MetaFrame XP(s,a,e) Feature Release 2/Service Pack 2). The error and warning thresholds for the monitor can be set on one or more Citrix Server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Citrix Server Monitor Overview" on page 413

The Add/Edit Citrix Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Choose the server where the Citrix Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

ColdFusion Server Monitor Settings

Description	Monitor the availability of an Allaire ColdFusion server (versions 4.5x) on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more ColdFusion server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"ColdFusion Server Monitor Overview" on page 415

The Add/Edit ColdFusion Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the ColdFusion Server you want to monitor is running. You cannot directly edit this field. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see "Configure SiteScope to Monitor a Remote Windows Server" on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

COM+ Server Monitor Settings

Description	The Com+ Server Monitor monitors the performance of software components registered and running on Microsoft COM+ servers. When you specify the host and port number of this probe instance, SiteScope retrieves all the functions running on the COM+ server, for your monitoring selection. Error and warning thresholds for the monitor can be set on one or more function measurements. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. Monitors must be created in a group in the monitor tree.
Useful Links	"COM+ Server Monitor Overview" on page 416

The Add/Edit Com+ Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
COM+ Probe Host Name	Enter the host name of the COM+ Probe.
COM+ Probe Port Number	Specify the port number of the COM+ Probe. The installation default for the probe is at port 8008.
Authorization User Name	(Optional) User name for authorization to the probe.
Authorization Password	(Optional) Password for authorization to the probe.

GUI Element	Description
HTTP Proxy	(Optional) A proxy server can be used to access the probe. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the probe, enter the name here. Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the probe, enter the password here.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status. **Note:** Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with a Timeout value of more than 60 seconds to allow the server to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.

Dynamo Application Server Monitor Settings

Description	Allows you to monitor the availability of an ATG Dynamo platform. The error and warning thresholds for the monitor can be set on one or more Dynamo Application Server Monitor performance statistics via SNMP. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Dynamo Application Server Monitor Overview" on page 417

The Add/Edit Dynamo Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.
Index	Enter the index of the SNMP object you want to check with this monitor. Non-table object IDs have an index of 0 (zero).

GUI Element	Description
Community	Enter the community that the above SNMP object belongs to. You may need to consult with your network administrators about what community names are active in your network environment. **Default value:** public
Host Name	Enter the IP address or host name of the Dynamo Server to be monitored along with the port that server is answering on. If the SNMP agent for the Dynamo server is answering on a port other than the default port, you must include the port number as part of the host name address. **Default value:** 8870

Advanced Settings (Monitor Specific)

GUI Element	Description
Retry Delay	Enter the time, in seconds, for SiteScope to wait before retrying a request.
Timeout	Enter the total time, in seconds, that SiteScope should wait for a successful reply from the Dynamo server. If a reply is not received in the time indicated, the monitor returns a timeout error.

F5 Big-IP Monitor Settings

Description	Use to monitor the administrative and performance statistics for an Apache server. Allows you to monitor the statistics of a F5 Big-IP load balancing device using SNMP. The error and warning thresholds for the monitor can be set on one or more load balancer statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"F5 Big-IP Monitor Overview" on page 418

The Add/Edit F5 Big-IP Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Enter the name of the server you want to monitor.
SNMP Version	Select the version of SNMP to use when connecting.
Community	Enter the community string (valid only for version 1 or 2 connections).
SNMP V3 Authentication Type	Select the type of authentication to use for version 3 connections.
SMNMP V3 Username	Enter the user name for version 3 connections.
SMNMP V3 Authentication Password	Enter the authentication password to use for version 3 connections.

GUI Element	Description
SMNMP V3 Privacy Password	Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.
SMNMP V3 Context Engine ID	Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.
SMNMP V3 Context Name	Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.
Timeout	Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.
Retries	Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.
Port	Enter the port to use when requesting data from the SNMP agent. The default of 161 is the port on which an SNMP agent is typically listening.
Starting OID	Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered in this field. The default value is 1, which is commonly used and applicable to most applications. You should edit this field 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 in this field.
MIB File	Select either the F5 MIB file or **All MIBs**. Selecting the F5 MIB file displays only those objects that are described within that MIB file. Selecting **All MIBs** 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.

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Counter Calculation Mode	Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. The available calculations are: ➤ a simple delta of the current value from the previous value, OR ➤ a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements **Note:** 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.

IIS Server Monitor Settings

Description	Allows you to monitor the availability and server statistics of a Microsoft IIS server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more IIS server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"IIS Server Monitor Overview" on page 418

The IIS Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the F5 Big-IP Server you want to monitor is running. You cannot directly edit this field. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see "Configure SiteScope to Monitor a Remote Windows Server" on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

iPlanet Server Monitor Settings

Description	Allows you to monitor the availability of SunONE/iPlanet and Netscape servers. The error and warning thresholds for the monitor can be set on one or more Netscape server performance statistics or HTTP response codes. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"iPlanet Server Monitor Overview" on page 419

The iPlanet Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Counters	Choose the server performance parameters and counters you want to check with this monitor. The list to the right of this item displays the available parameters and counters and those currently selected for this monitor. **Note:** ➤ Select only those counters that are applicable to the server version you want to monitor. ➤ Do not edit the order of the counters in the selected counter text box. The counters must be maintained in the order they appear in the **choose counter** selection page.

GUI Element	Description
URL	Select the URL you want to verify with this monitor. This URL should be the URL to the applicable server monitor statistics Web page for the server version you want to monitor. For iPlanet 4.1 servers this usually has the format http://servername:adminport/https-serveraddress/bin/sitemon?doit. For iPlanet 6.0 servers, the URL of the monitor statistics Web page has the format http://servername:adminport/https-instanceserveraddress/bin/instance-app/pageStats.jsp?pollInterval=15&vsname=All where <pageStats.jsp> is replaced with the file reference for the specific statistics page you want to monitor (see the list of counters). **Note:** The **servername:port** and **serveraddress** are not necessarily identical depending on if you access the administrator server pages locally or remotely. The SiteScope iPlanet Server Monitor generally needs to be configured using the full **serveraddress** and not the https-admserv syntax. Normally you can find the **serveraddress** in the **Select a Server** box on the main administration Web page. **Note:** (For Advanced Users Only) The iPlanet Server Monitor can be used to monitor other server products in the SunONE product line that make their performance statistics available via a server monitor statistics Web page. To monitor other products you need to know the URL of the access log or administration Web page for that product version. You need to modify the regular expression in the _netscapeRegExp= entry of the SiteScope **master.config** file and add any additional counter strings to the **SiteScope/templates.applications/counters.iplanet** file to extract the applicable values from the administration logs.

Advanced Settings (Monitor Specific)

GUI Element	Description
Authorization User Name	If the server you want to monitor requires a name and password for access, enter the name in this box.
Authorization Password	If the server you want to monitor requires a name and password for access, enter the password in this box.
HTTP Proxy	Optionally, a proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status. **Note:** Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Timeout value of more than 60 seconds to allow the server to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.

News Monitor Settings

Description	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. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"News Monitor Overview" on page 422

The News Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
News Server	Enter the IP address or the name of the news server that you want to monitor. **Example:** 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. **Example:** news.thiscompany.com:7777
News Groups	Optionally enter one or more news groups to be checked, separated by commas. Each of these news groups are checked for the current number of articles available in that news group. The reading of the monitor is the sum of articles available for each of the specified news groups.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The number of seconds that the News monitor should wait for all of news transactions to complete before timing-out. Once this time period passes, the News monitor logs an error and reports an error status.
User Name	If your News server requires authorization, enter a valid user name here.
Password	If your News server requires authorization, enter a valid password here.
Connect From	The name or IP address of the server that connects to the News monitor.

Oracle 9i Application Server Monitor Settings

Description	The Oracle 9i Application Server Monitor allows you to monitor the availability and performance statistics of a Oracle9i Application Server. The error and warning thresholds for the monitor can be set on one or more Oracle9i server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Oracle9i Application Server Monitor Overview" on page 423

The Oracle 9i Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
URL	Enter the server administration URL for the server you want to monitor. The URL is usually in the format: http://server:port/webcacheadmin?SCREEN_ID=CGA.Site.Stats& ACTION=Show.
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Authorization User Name	If the server you want to monitor requires a name and password for access, enter the name in this box.
Authorization Password	If the server you want to monitor requires a name and password for access, enter the password in this box.
HTTP Proxy	Optionally, a proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.

Oracle10g Application Server Monitor Settings

Description	The Oracle10g Application Server Monitor allows you to monitor the availability and performance statistics of an Oracle10g Application Server. The error and warning thresholds for the monitor can be set on one or more Oracle10g server performance statistics Monitor allows you to monitor the availability and performance statistics of an Oracle10g Application Server. The error and warning thresholds for the monitor can be set on one or more Oracle10g server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Oracle10g Application Server Monitor Overview" on page 424

The Oracle10g Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Authorization User Name	If the server you want to monitor requires a name and password for accessing, enter the name in this box.
Password	If the server you want to monitor requires a name and password for accessing, enter the password in this box.
Proxy Server	Optionally, a proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.

GUI Element	Description
Proxy Server User Name	If the proxy server requires a name and password to access the server, enter the name here. Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, enter the password here. Your proxy server must support Proxy-Authenticate for these options to function.
Host Name	Enter the server administration URL for the server you want to monitor.
Metric Type	Enter the type of metrics to monitor. Options are App Server (OC4J) and Web Server (DMS).
Port	Enter the server port for the server you want to monitor. Default value is 7201 and is configured in the dms.conf file.
Secure Server	Select this option to use a secure server.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.

Radius Monitor Settings

Description	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. Use this page to add a monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Radius Monitor Overview" on page 424

The Add/Edit Radius Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
RADIUS Server	Enter the IP address or the name of the RADIUS server that you want to monitor. **Example:** 206.168.191.21 or radius.thiscompany.com
Secret Phrase	Enter the secret used to encrypt all requests to this RADIUS server.
User Name	Enter the user name to authenticate.
Password	Enter the password to authenticate.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The number of seconds that the Radius monitor should 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.
Port	Choose the TCP port used by the RADIUS server. **Default value:** 1645
Match Content	Enter a string of text to check for in the response. If the text is not contained in the response, the monitor displays the message **no match on content**. 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. **Example:** / \d\d/ or /size \d\d/i **Note:** The search is case sensitive.

SAP CCMS Monitor Settings

Description	The SAP CCMS Monitor allows you to monitor the performance of your SAP R/3 System landscape in a centralized manner using SAP CCMS interface. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. Monitors must be created in a group in the monitor tree.
Useful Links	"SAP CCMS Monitor Overview" on page 426

The Add/Edit SAP CCMS Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Application Server	Enter the address of the SAP server you want to monitor.
SAP Client	Enter the Client to use for connecting to SAP.
System Number	Enter the System number for the SAP server.
Authorization User Name	Enter the user name required to connect to the SAP server.
Authorization Password	Enter the password required to connect to the SAP server.
SAP Router String	If your connection is being made through a router, enter a router address string, otherwise leave it blank. 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.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor. This tree more or less matches the hierarchy of Monitoring Tree Elements displayed in the Monitoring Tree that is shown in the SAP GUI with transaction RZ20. However, the SiteScope browse tree may show more or less information than RZ20 depending on the authorization level of the user name you specified for this monitor.

SAP CCMS Alerts Monitor Settings

Description	The SAP CCMS Alerts Monitor allows you to read and complete alerts from the SAP CCMS Alerts monitors. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. Monitors must be created in a group in the monitor tree.
Useful Links	"SAP CCMS Alerts Monitor Overview" on page 429

The Add/Edit SAP CCMS Alerts Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Application Server	Enter the host name/IP address of the SAP server you want to monitor.
SAP Client	Enter the Client to use for connecting to SAP.
System Number	Enter the System number for the SAP server.
Authorization User Name	Enter the user name required to connect to the SAP server. This user must have authorization to access CCMS metrics.
Authorization Password	Enter the Password required to connect to the SAP server.
SAP Router String	If your connection is being made through a router, enter a router address string, otherwise leave it blank. 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.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

SAP Java Web Application Server Monitor Settings

Description	The SAP Java Web Application Server Monitor allows you to monitor the availability and server statistics for SAP Java Web Application server cluster. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	This monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running. Monitors must be created in a group in the monitor tree.
Useful Links	"SAP Java Web Application Server Monitor Overview" on page 432

The Add/Edit SAP Java Web Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Application Server	Enter the address of the SAP Java Web Application Server you want to monitor.
Port	Enter the port number of the SAP Java Web Application Server you want to monitor. **Default value:** 50004
Authorization User Name	Enter the user name required to connect to the SAP server.
Authorization Password	Enter the Password required to connect to the SAP server.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor. These counters are received dynamically from the JMX.

SAP Work Processes Monitor Settings

Description	The SAP Work Processes Monitor allows 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. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. Monitors must be created in a group in the monitor tree.
Useful Links	"SAP Work Processes Monitor Overview" on page 434

The Add/Edit SAP Work Processes Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Application Server	Enter the address of the SAP server you want to monitor.
SAP Client	Enter the Client to use for connecting to SAP.
System Number	Enter the System number for the SAP server.
Authorization User Name	Enter the user name required to connect to the SAP server.
Authorization Password	Enter the password required to connect to the SAP server.
SAP Router String	If your connection is being made through a router, enter a router address string, otherwise, leave it blank. 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.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Siebel Application Server Monitor Settings

Description	The Siebel Application Server Monitor (previously know as the Siebel Server Manager Monitor) uses the Siebel Server Manager client to monitor Object Manager components and task information on Siebel application servers. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. Monitors must be created in a group in the monitor tree.
Useful Links	"Siebel Application Server Monitor Overview" on page 437

The Add/Edit Siebel Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Script Server	Select or enter the remote Windows or UNIX machine where the Server Manager (srvrmgr) script is installed. The method of connection is either SSH or Telnet (but not Microsoft NetBios). For NetBios, choose this server and map the drive.
Siebel Host Name	This field is required if you are doing either of the following: ➤ **Doing process monitoring.** In this case you must define a Remote Definition to the target Siebel machine whose Siebel processes are to be monitored. Specify in this field the **Host Server Name** of the Siebel Remote definition (not the **Title**). This is the **NT Server Address** field for NT Remotes or **Server Address** field for UNIX Remotes. ➤ **Reporting monitor data to an installation of HP Business Availability Center.** In this case the value entered is used as a text identifier describing the target Siebel server that this monitor is monitoring. This text descriptor is used to identify the Siebel server when the monitor data is viewed in an HP Business Availability Center report. The field is optional only if the Script Server field is already specified to be the target Siebel server.
Application Server	Enter the Siebel server name or address.
Gateway Server	Enter the Gateway server name or address.
Enterprise Server	Enter the Enterprise server name or address.
User	Enter the user name for the Siebel Server Manager client.
Password	Enter the password for the Siebel Server Manager client.

GUI Element	Description
Script Path	The full path to the Siebel Server Manager executable directory relative to the machine chosen above. **Example:** E:\sea704\client\BIN
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Siebel Tasks Time Window	Specify a time window in which tasks are monitored on the Siebel application server. If the task start time is within the time window (for example, 20 minutes), the task is monitored. The time window is calculated according to the formula: time window = (current time – property value). Enter 0 to monitor every task on the Siebel application server, regardless of its start time. **Default value:** 60 minutes

Siebel Log File Monitor Settings

Description	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. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. Monitors must be created in a group in the monitor tree.
Useful Links	"Siebel Log File Monitor Overview" on page 440

The Add/Edit Siebel Log File Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The Siebel server where the log files you want to monitor is running. You cannot directly edit this field. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see "Configure SiteScope to Monitor a Remote Windows Server" on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.
Log File Directory	Enter the pathname to the log directory you want to monitor. To monitor log files on a remote Windows NT/2000 server through NetBIOS, specify a UNC path to the remote directory. **Example:** \\remoteserver\logFileDirectory If you are using SSH as a connection method to the remote NT server you need to select the **java library** and **ssh1** options for that remote.

GUI Element	Description
File Name	Select the log files that you want to monitor. A regular expression must be used to specify multiple files. The search is not recursive and only matches files listed within the log file directory. **Note:** Selecting too many log files to monitor can significantly degrade SiteScope performance.
Severity	Select the severity level of entries to consider for matching. Entries that have the correct event type/subtype and have an equal or greater severity are matched. Those entries with lesser severity are ignored.
Event Type	Select the matching event type or subtype. The monitor reports how many log entries were found of the specified type.
Log-Entry Content Match	(Optional) You may specify an additional text string or regular expression to further narrow down the matched log entries. This match expression is run against the content returned from the initial Severity and Event Type match. You use this option to find only those log entries with the selected severity an event type that meet this additional match criteria.
Search from Start	Select 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. The following table describes the options for this setting: ➤ **Off.** Check only newly-added records, starting at the time that the monitor was created (not when the file was created). ➤ **On.** Always check the contents of the whole file. **Note:** Monitoring large numbers of log files with this option may use large amounts of memory and CPU time. This can degrade SiteScope server performance. **Default value:** Off

Siebel Web Server Monitor Settings

Description	The Siebel Web Server Monitor allows you to use SiteScope to monitor statistical and operational information about a Siebel server by way of the Siebel Web server plug-in. You can use this monitor to watch Siebel server login session statistics and gauge the performance of the Siebel server Object Managers and database. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. Monitors must be created in a group in the monitor tree.
Useful Links	"Siebel Web Server Monitor Overview" on page 441

The Add/Edit Siebel Web Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Application URL	Enter the URL of the Web plug-in server stats page for the application you want to monitor. **Example:** http://siebelsrv/service/_stats.swe If the Siebel Web server is configured to support verbose mode, you can also use http://siebelsrv/service/_stats.swe?verbose=high to include information on Locks and Current Operations Processing for the Siebel server.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Authorization User Name	Enter the user name to access the Web server stats page.
Authorization Password	Enter the password for accessing the Web server stats page.
HTTP Proxy	If you are using a proxy to access the Siebel server, enter the proxy server and port to use. **Example:** proxy.SiteScope.com:8080
Proxy Server User Name	Enter the proxy user name if the proxy server requires authorization.
Proxy Server Password	Enter the proxy password if the proxy server requires authorization. If access to the Siebel Web Server site is controlled by a centralized authorization and authentication access control system, the following fields are used to submit information to a HTML/CGI enabled authentication system. You can determine if authentication is required by trying to access the Web plug-in server stats page using a Web browser outside of SiteScope. If an HTML-based authentication form opens before you see the Siebel service statistics page, you need to use the following fields to access the Siebel Web server plug-in.
HTML Form-based Authentication Required	Check this option to have SiteScope submit HTML form-based authentication when accessing the Siebel Web server plug-in.
Authorization Form Name	When using HTML Form-based Authentication, this is the identifier of the authentication form within the Web page. The identifier is a number representing the place or order of the forms on an HTML page. **Example:** [1] is the first HTML <FORM> set, [2] is the second, and so on. The default is [1] since it assumes that the authentication information is entered into the first HTML <FORM> tag set on the page.

GUI Element	Description
Authorization Username Form Field	When using HTML Form-based Authentication, enter the user name that should be submitted to the access control system. This must be the user name that would be entered in the authentication form the same as if you were accessing the Siebel Web server plug-in manually using a Web browser.
Authorization Password Form Field	Enter the password that should be submitted to the access control system. This must be the password that would be entered in the authentication form when accessing the Siebel Web server plug-in manually using a Web browser.
Authorization Form Button	When using HTML Form-based Authentication, this is the identifier of the Submit button on the authentication form. The identifier is a number representing the place or order of the buttons on an HTML page. **Example:** [1] is the first HTML <INPUT TYPE=SUBMIT> button, [2] is the second, and so on. **Default value:** [1]

SilverStream Server Monitor Settings

Description	The SilverStream Server Monitor allows you to monitor the availability of an SilverStream server. The error and warning thresholds for the monitor can be set on one or more SilverStream server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	The monitor supports SilverStream versions 4.x. There is limited support for versions 5.0 and higher (includes only hits and bytes in the available counters). Monitors must be created in a group in the monitor tree.
Useful Links	"SilverStream Server Monitor Overview" on page 442

The Add/Edit SilverStream Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.
URL	Choose the URL you want to verify with this monitor. This URL should be the URL to the applicable server administration Web page. It usually has the format http://<servername>:<port>/SilverStream/Statistics. **Default value (port):** 80

Advanced Settings (Monitor Specific)

GUI Element	Description
Authorization User Name	If the server you want to monitor requires a name and password for access, enter the name in this box.
Authorization Password	If the server you want to monitor requires a name and password for access, enter the password in this box.
HTTP Proxy	(Optional) A proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, enter the name here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, enter the password here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.

SunONE Server Monitor Settings

Description	The SunONE Server Monitor allows you to monitor the availability of SunONE or iPlanet 6.x servers using the stats-xml performance metrics file (iwsstats.xml or nesstats.xml) facility. By providing the URL of this stats-xml file, SiteScope can parse and display all metrics reported in this file and allow you to choose those metrics you need to be monitored as counters. In addition, several derived counters are provided for your selection which measure percent utilization of certain system resources. Error and warning thresholds for the monitor can be set on one or more SunONE server performance statistics or HTTP response codes. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"SunONE Server Monitor Overview" on page 443

The Add/Edit SunONE Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Stats-XML URL	Specify the URL to the stats-xml file on the SunONE server you want to monitor. This is usually in the form http://server_id:port/stats-xml/<stats-xml-file> where <stats-xml-file> is **nesstats.xml** or **iwsstats.xml**.
Authorization User Name	Enter the user name of the SunONE server you want to monitor.

GUI Element	Description
Authorization Password	Enter the password of the SunONE server you want to monitor.
HTTP Proxy	(Optional) A proxy server can be used to access the server. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the server, enter the name here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, enter the password here.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status. **Note:** Depending on the activity on the server, the time to build the server monitor statistics Web page may take more than 15 seconds. You should test the monitor with an Timeout value of more than 60 seconds to allow the server time to build and serve the server monitor statistics Web page before the SiteScope monitor is scheduled to run again.

Tuxedo Monitor Settings

Description	The Tuxedo Monitor allows you to monitor the availability of an BEA Tuxedo server. The error and warning thresholds for the monitor can be set on one or more Tuxedo Monitor performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Tuxedo Monitor Overview" on page 444

The Add/Edit Tuxedo Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Enter the 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 pathname of the applicable server.
Port	Enter the port number for the Tuxedo server. The port number should match the port dedicated to the Tuxedo Workstation component (the WSL process). **Default value:** 65535
User	Enter the user name if required to access the Tuxedo server.
Password	Enter the Password if required to access the Tuxedo server.
Client Name	Enter an optional client name for the Tuxedo server.
Connection Data	Enter any extra or optional Connection Data to be used for connecting to the Tuxedo server. In some cases, this may be a hexadecimal number.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

UDDI Monitor Settings

Description	The UDDI Monitor checks the availability and round-trip response time of the UDDI server. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"UDDI Monitor Overview" on page 445

The Add/Edit UDDI Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Inquiry URL	Enter the UDDI server inquiry URL. **Example:** http://uddi.company.com/inquiry/
Business Name	Enter the business entity to search for in the UDDI server.

Advanced Settings (Monitor Specific)

GUI Element	Description
Max Businesses Number	The maximum allowed business entities to receive from the UDDI server (1–200). **Default value:** 10

VMware Performance Monitor Settings

Description	The VMware Performance Monitor enables you to monitor performance statistics of the VMware infrastructure for various server applications. The supported applications include VirtualCenter 2.0.x, ESX Server 3.0.x, and others. The monitor supports monitoring both single VMware ESX server installations and ESX server clusters managed by VMware Virtual Centers. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	The following are the requirements for monitoring: ➤ The monitored VI server or ESX server cluster must be directly accessible by the SiteScope server (no proxy involved). ➤ The VI server or ESX server cluster provides connection either by http or by https (depending on the VI server configuration). If https is used, server certificate must be imported to the SiteScope. Monitors must be created in a group in the monitor tree.
Useful Links	"VMware Performance Monitor Overview" on page 446

The Add/Edit VMware Performance Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Connection URL	Select the VMware infrastructure for the server you want to monitor. The format of the URL is: <protocol>://<server_name>/sdk ➤ <protocol> is either http or https. ➤ <server_name> is the name of the VI server.
User Name	The user name of the VMware web service's administrator.
Password	The password of the VMware web service's administrator.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Socket timeout	Enter the number in milliseconds that the VMware monitor should wait for data from a server during a single data request. Once the socket timeout period elapses, the monitor logs an error and reports the error status. **Note:** ➤ The socket timeout value must be larger than 0. ➤ The value of zero is interpreted as an infinite timeout. **Default value**: 600000

WebLogic Application Server Monitor Settings

Description	The WebLogic Application Server Monitor allows you to monitor the statistics of a WebLogic version 6 through 8 servers. For WebLogic Application Server version 9, a JMX monitor should be used. The error and warning thresholds for the monitor can be set on one or more Application Server statistics. WebLogic Application Server Monitors cannot be used to monitor WebLogic 9.x servers. To monitor these servers, use a JMX monitor. For further details, see "Creating a JMX Monitor for a WebLogic 9.x Server" on page 489. If you are using a WebLogic 9.x server, this chapter is not relevant. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"WebLogic Application Server Monitor Overview" on page 448

The Add/Edit WebLogic Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Target	Enter the name of the server where WebLogic is running.
Server	Enter the address of the server where WebLogic is running.
Port Number	Enter the port number that the WebLogic server is responding on. **Default value:** 7001
User Name	Enter the user name required to log into the WebLogic server.
Password	Enter the password required to log into the WebLogic server.
Secure Server	Select this box if you are using a secure server connection option. If you select this option, you must enter the applicable port number used by the WebLogic server for secure connections. **Default value:** 7002
WLCipher Jar File	For some versions of WebLogic Server, you need to install a copy of the wlcipher.jar file from the WebLogic server onto the SiteScope server to enable monitoring over SSL. Enter the absolute path to the file on the SiteScope machine in this field. **Example:** C:\bea\weblogic81\server\lib\wlcipher.jar **Note:** This option is for use only with the **Secure Server** (SSL) option.

GUI Element	Description
WebLogic License File	You use this field only when you want to enable the Secure Server (SSL) option. Enter the absolute path to the BEA license file that was copied to the SiteScope machine. **Example:** C:\bea\license.bea
Location of JVM	Enter the full path to the Java Virtual Machine (JVM) in which the WebLogic monitoring process should be run. For monitors that do not use the Secure Server option, this is not required. 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. **Example:** C:\j2sdk1.4.1\jre\bin\javaw.exe
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status. **Default value:** 180 It is recommended not to change the default value so that performance is not adversely affected.
WebLogic Jar File	Enter the absolute path name 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. **Example:** c:\bea\weblogic7\ebcc\lib\ext\weblogic.jar 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.

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

WebSphere Application Server Monitor Settings

Description	The WebSphere Application Server Monitor allows you to monitor the availability and server statistics of an IBM WebSphere Application Server 3.5.x, 4.x, 5.x, and 6.x. The error and warning thresholds for the monitor can be set on one or more WebSphere Application Server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"WebSphere Application Server Monitor Overview" on page 451

The Add/Edit WebSphere Application Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Target	Enter the logical name of the server you want to monitor. If this box is left empty, the hostname entered above is used.
Server	Choose the server where the WebSphere Application Server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.
Port Number	Enter the port number for the SOAP.
User Name	Enter the user name to access the WebSphere Application Server if one has been configured.
Password	Enter the password to access the WebSphere Application Server if one has been configured.
Security Realm	Only relevant for WebSphere 3.5 users. Specify the security realm of the WebSphere application server.
Version	Enter the version of the WebSphere application you are monitoring.
WebSphere Directory	➤ For 3.x: Enter the path to a WebSphere 3.5x Directory. The directory you enter here should contain at least a valid Admin Client installation. ➤ For 6.x: Enter the path to the AppServer directory.
Client Properties File	For version 6.x, enter **SOAP.client.props**.
Classpath	(Optional) Enter additional classpath variables that are to be used by the WebSphere JVM running on the SiteScope machine.

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

In WebSphere Application Server version 6.x, you can enable global security by configuring the properties below:

GUI Element	Description
Trust Store	This is the full directory path of file **DummyClientTrustFile.jks**. This file is in the client monitor directory on the SiteScope machine. The default path is **C:\WebSphere\AppServer\profiles\default\etc**.
Trust Store Password	This is the password for the SSL trust store file. **Default value:** WebAS
Key Store	This is the full directory path of file **DummyClientKeyFile.jks**. This file is in the client monitor directory on the SiteScope machine. **Default value:** C:\WebSphere\AppServer\profiles\default\etc
Key Store Password	This is the password for the SSL key store file. **Default value:** WebAS The values for Trust Store, Trust Store Password, Key Store, and Key Store Password are automatically configured and can be found in the following directories: ➤ on Windows platform, in <drive>:\WebSphere\AppServer\etc\ ➤ on Solaris platform, in /opt/WebSphere/AppServer/etc/ ➤ on Linux platform, in /opt/IBMWebAS/etc/ For more information about Key Store passwords, refer to the IBM Information Center (http://publib.boulder.ibm.com/infocenter/wasinfo/v4r0/index.jsp?topic=/com.ibm.websphere.v4.doc/wasa_content/050703.html) and search for SSL configuration.

WebSphere MQ Status Monitor Settings

Description	The WebSphere MQ Status Monitor allows you to monitor the performance attributes of MQ Objects (channels and queues) on MQ Servers v5.2 and later. Both performance attributes and events for channels and queues can be monitored. This monitor was formerly known as MQSeries. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. Monitors must be created in a group in the monitor tree.
Useful Links	"WebSphere MQ Status Monitor Overview" on page 455

The Add/Edit WebSphere MQ Status Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
MQ Server Name	Specify the host name of the MQ Server you want to monitor. Enter the network name of the server or the IP address of the server. **Example:** mqmachinename
MQ Server Port	Specify the port number of the target MQ Server. **Default value:** 1414

GUI Element	Description
Server Connection Channel	Enter the name of the server connection channel of the target MQ server. Check with the MQ Server administrator for the name syntax of the server connection channel.
Queue Manager	Enter the name of the queue manager whose queues or channels are to be monitored.
Alternate Queue Manager	(Optional) You can enter an alternate queue manager name that has been set up to forward its events to the primary queue manager specified above if you are also interested in monitoring those events.
Selected Measurements	The **Get Measurements** button allows you to add or delete counters for the monitor. Click this button after you have specified all the server information above. There are two primary window panes on the Measurement Selection page: ➤ **Available Measurements.** A browse window which displays available MQ queue instances and channel instances, and counters to choose from. You must first select either Queue or Channel Objects to work with in the **Objects** drop-down list. Once an object is selected, a connection to the MQ server is made, using the server information provided in the previous page. A list of available queues or channels is displayed, both system and user instances, depending on the object type selected. After pressing the **Add** button, any number of instances and counters you select via check boxes are combined into individual monitoring counters and listed in the Selected Measurements window. ➤ **Selected Measurements.** Lists the counters you have selected to be monitored from pressing the **Add** button. The **X** check box preceding each counter allows you to delete the counter.

Advanced Settings (Monitor Specific)

GUI Element	Description
Channel Status Code Scheme	Select a reporting schemes for Channel Status Code values: ➤ **Use HP coding scheme.** Report the actual or original channel status codes as documented in the IBM MQ literature. ➤ **Use IBM MQ coding scheme.** Report channel status codes in ascending values that are directly proportional to the health of the channel. SiteScope reports a channel status value from 0 (least healthy) to 6 (healthiest). For details, see "Channel Status Codes" on page 457.

WebSphere Performance Monitor Settings

Description	The WebSphere Performance Monitor to monitor the server statistics of IBM WebSphere Server (versions 3.0x, 3.5, 3.5.x, and 4.0) via a WebSphere Performance Servlet. The error and warning thresholds for the monitor can be set on one or more performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"WebSphere Performance Servlet Monitor Overview" on page 460

The Add/Edit WebSphere Performance Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Enter the server you want to monitor. On UNIX servers, enter the full pathname of the server. You are also asked to enter the URL to the performance servlet as installed on the WebSphere server and the port number that is to be used to access the server. For WebSphere versions 3.x.x, the URL can be viewed via the Servlet Properties page in the WebSphere Admin Console. For WebSphere version 4.0, the URL normally has the form: http://<server:port_number:>/wasPerfTool/servlet/perfservlet.
Secure Server	Enter the secure server you want to monitor.
Target	Enter the logical name of the server that is the target of this monitor instance. If you leave this field empty, the hostname is used. Depending on the deployment of the WebSphere application in your infrastructure, this may be the same as the **Server** selected above.
Port	Enter the port number to the WebSphere server you want to monitor. **Default:** 80 for non-secure server and 443 for secure server.
Servlet URL	URL of the performance servlet. For WebSphere 4.0, the default URL is /wasPerfTool/servlet/perfservlet. On earlier versons, the URL is chosen during the installation of the servlet. For WebSphere 6.0 and later, use the URL: /wasPerfTool/servlet/perfservlet?version=5. In either case, the URL can be found in the Servlet properties page of the Admin Console.

GUI Element	Description
Authorization User Name	If the URL requires authorization, enter the user name here.
Password	If the URL requires authorization, enter the password here.
Proxy Server User Name	If the proxy server requires a name and password to access the server, enter the name here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the server, enter the password here.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	Enter the time, in seconds, that the monitor should wait for a response from the Performance Servlet. If a response is not received within the interval of the timeout, the monitor reports a timeout error.
Refresh Selected Metrics Frequency	Select a time interval at which the WebSphere server should update the metrics that are requested by this monitor. This value should be equal to or less than the **Frequency** time interval for the monitor.

36

Database Monitors User Interface Settings

This chapter includes the pages and dialog boxes that enable you to add and edit SiteScope monitors.

DB2 Monitor Settings

Description	Monitors the availability and performance statistics of an IBM DB2 database versions 6.x and 7.x. The 8.x versions of DB2 are not currently supported. The error and warning thresholds for the monitor can be set on one or more DB2 server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"DB2 Monitor Overview" on page 463

The Add/Edit DB2 Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Enter the address or name of the server where the DB2 database is running.
Node Name	Enter the DB2 database node name that you want to monitor. **Example:** DB2 is a default node created by DB2 installation.
User Name	Enter the DB2 database user name to be used to access the DB2 server. This is usually a DB2 administrator user name.
Password	Enter the password for the user specified above.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

DB2 8.x Monitor Settings

Description	Monitors the availability and performance statistics of an IBM DB2 database for versions 8.x. The error and warning thresholds for the monitor can be set on up to ten DB2 server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"DB2 8.x Monitor Overview" on page 465

The Add/Edit DB2 8.x Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
DB2 Server	Enter the address or name of the server where the DB2 8.x database is running.
Port	The port on which the DB2 8.x database accepts connections. **Default value:** 5000
Database	Enter the DB2 database node name that you want to monitor. **Example:** DB2 is the default node name created by DB2 installation.
Database User Name	Enter the DB2 database user name to be used to access the DB2 server. This is usually a DB2 administrator user name.
Database Password	Enter the password for the user specified above.

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Partition	Partition to monitor. **Example**: -1 is the current partition; -2 is all partitions.
Calculate Rate	Select to calculate rates for counter values rather than the actual values returned from the monitored server. **Example**: If a counter counts logins and every second an average of two users log in to the database, the counter keeps growing. Selecting this option, the monitor displays the value 2, which means 2 user logins per second.

Database Connection Settings

Description	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, dynamic updates, and database monitors (Oracle database, Database Counter, Database Query, DB2 8.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.
Important Information	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.
Useful Links	"JDBC Global Options" on page 232

The Database Connection Settings include the following elements:

GUI Element	Description
Use Connection Pool	If this check box is checked, SQL connection sharing is enabled. This means that you use a connection pool rather than open and close a new connection for each monitor query. **Default setting:** Enabled
Physically Close if idle connection count exceeds	This is the maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool. **Default value:** 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. **Default value:** 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 feature. If your SQL driver does not support this feature, this parameter is ignored. **Default value:** 1 minute

Database Counter Monitor Settings

Description	The Database Counter Monitor allows you to monitor the availability of any database through a JDBC driver. The error and warning thresholds for the monitor can be set on one or more database server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. Monitors must be created in a group in the monitor tree.
Useful Links	"Database Counter Monitor Overview" on page 466

The Add/Edit Database Counter Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Database Connection URL	Enter the connection URL to the database you want to connect to. The syntax is jdbc:oracle:thin:@<server name or IP address>:<database server port>:<sid>. **Example:** To connect to the ORCL database on a machine using port 1521 use: jdbc:oracle:thin:@206.168.191.19:1521:ORCL. The colon (:) and @ symbols must be included as shown. **Note for using Windows Authentication:** If you want to access the database using Windows authentication, enter jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>; AuthenticationMethod=type2 as the connection URL, and com.mercury.jdbc.sqlserver.SQLServerDriver as your database driver. Leave the **Database User Name** and **Database Password** boxes empty, since the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.
Query	Enter a SQL query that returns at least two columns of data. The values in the first column of data are interpreted as the labels for the entries in the each row. The values in the first row are treated as labels for each entry in the column.
Database User Name	Enter the user name that SiteScope should use to connect to the database.
Database Password	Enter the password for the user name that SiteScope should use to connect to the database.
Database Driver	Enter the driver used to connect to the database. **Example:** org.postgresql.Driver

GUI Element	Description
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
DB Machine Name	The identifier for the target database server, as it should be reported to HP Business Availability Center.
Divisor Query	A SQL query that returns a single numeric value. The value of each counter is calculated by dividing the counter value as retrieved from the database divided by the Divisor Query value.
No Cumulative Counters	Selecting this check box 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).
No Divide Counters	Selecting this check box 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. The divisor is either taken from the Divisor Query, or it is the elapsed time in seconds since the previous monitor run.

Database Connection Settings

Description	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, dynamic updates, and database monitors (Oracle database, Database Counter, Database Query, DB2 8.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.
Important Information	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.
Useful Links	“JDBC Global Options” on page 232

The Database Connection Settings include the following elements:

GUI Element	Description
Use Connection Pool	If this check box is selected, SQL connection sharing is enabled. This means that you use a connection pool rather than open and close a new connection for each monitor query. This option is selected by default.
Physically Close if idle connection count exceeds	This is the maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool. **Default value:** 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. **Default value:** 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 feature. If your SQL driver does not support this feature, this parameter is ignored. **Default value:** 1 minute

Database Query Monitor Settings

Description	Checks that a database is working correctly by connecting to it and performing a query. Optionally, it can check the results of a database query for expected content. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Database Query Monitor Overview" on page 469

The Add/Edit Database Query Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Database Connection URL	Enter a URL to a Database Connection. One way to create a database connection is to use ODBC to create a named connection to a database. **Example:** First use the ODBC control panel to create a connection called test. Then, enter jdbc:odbc:test in this box as the connection URL. **Note for using Windows Authentication:** If you want to access the database using Windows authentication, enter jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>; AuthenticationMethod=type2 as the connection URL, and com.mercury.jdbc.sqlserver.SQLServerDriver as your database driver. Leave the **Database User Name** and **Database Password** boxes empty, since the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.
Database Driver	Enter the java class name of the JDBC database driver. The default driver uses ODBC to make database connections. SiteScope uses the same database driver for both primary and backup database connections. If a custom driver is used, the driver must also be installed in the <**SiteScope root directory**>**/WEB-INF/lib** directory. **Default value:** sun.jdbc.odbc.JdbcOdbcDriver

GUI Element	Description
Database User Name	Enter the user name used to log in to the database. If you are using Microsoft SQL server and the default driver (Sun Microsystem JDBC-ODBC bridge driver, sun.jdbc.odbc.JdbcOdbcDriver), you can leave this blank and choose NT Authentication when you setup the ODBC connection. With NT Authentication, SiteScope connects using the login account of the SiteScope service. **Note:** The specified user name must have privileges to run the query specified for the monitor.
Database Password	Enter a password used to login to the database. If you are using Microsoft SQL server and the default driver (Sun Microsystem JDBC ODBC bridge driver (sun.jdbc.odbc.JdbcOdbcDriver), you can leave this blank and choose NT Authentication when you create the ODBC connection. With NT Authentication, SiteScope connects using the login account of the SiteScope service.
Query	Enter the SQL query to test. **Example:** select * from sysobjects

Advanced Settings (Monitor Specific)

GUI Element	Description
Match Content	Enter a string of text to check for in the query result. If the text is not contained in the result, the monitor displays no match on content. This works for XML tags as well. You may also perform a Perl regular expression match by enclosing the string in forward slashes, with an i after the trailing slash indicating case-insensitive matching. **Example:** /href=Doc\d+\.html/ or /href=doc\d+\.html/i 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. **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. **Note:** The search is case sensitive.
File Path	Enter the name of the file that contains the query you want to run. The file should be in a simple text format. Use this feature as an alternative to the Query text box in the Main Settings pane for complex queries or queries that change and are updated by an external application.

GUI Element	Description
Column Labels	Enter the field labels for the two columns returned by the query, separated by a **,** (comma). These column labels are used as data labels in SiteScope reports for Database Query Monitors. **Note:** The field labels should be two of the labels that are returned by the Query string entered above.
DB Machine Name	If you are reporting monitor data to an installation of HP Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in an HP Business Availability Center report. **Note:** Use only alphanumeric characters for this entry. You can enter the name of the monitored server or a description of the database.

Database Connection Settings

Description	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, dynamic updates, and database monitors (Oracle database, Database Counter, Database Query, DB2 8.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.

Important Information	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.
Useful Links	"JDBC Global Options" on page 232

The Database Connection Settings include the following elements:

GUI Element	Description
Use Connection Pool	If this check box is checked, SQL connection sharing is enabled. This means that you use a connection pool rather than open and close a new connection for each monitor query. This option is checked by default.
Physically Close if idle connection count exceeds	This is the maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool. **Default value:** 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. **Default value:** 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 feature. If your SQL driver does not support this feature, this parameter is ignored. **Default value:** 1 minute

LDAP Monitor Settings

Description	Verifies that a Lightweight Directory Access Protocol (LDAP) server is working correctly by connecting to it and performing a simple authentication. Optionally, it can check the result for expected content. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"LDAP Monitor Overview" on page 478

The LDAP Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
LDAP Service Provider	Enter the constant that holds the name of the environment property for specifying configuration information for the service provider to use. The value of the property should contain a URL string (for example, ldap://somehost:389). 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.

GUI Element	Description
Security Principal	Enter the constant that holds the name of the environment property for specifying the identity of the principal for authenticating the caller to the service. The format of the principal depends on the authentication scheme. If this property is unspecified, the behavior is determined by the service provider. This should be of the form uid=testuser,ou=TEST,o=mydomain.com.
Security Credential	Enter the constant that holds the name of the environment property for specifying the credentials of the principal for authenticating the caller to the service. The value of the property depends on the authentication scheme. For example, it could be a hashed password, clear-text password, key, certificate, and so on. If this property is unspecified, the behavior is determined by the service provider.

Advanced Settings (Monitor Specific)

GUI Element	Description
Content Match	Enter a string of text to check for in the query result. If the text is not contained in the result, the monitor displays no match on content. The search is case sensitive. This works for XML tags as well. 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. **Example:** /href=Doc\d+\.html/ or /href=doc\d+\.html/i 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. **Example:** /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.

GUI Element	Description
Object Query	Use this box to enter an object query to look at a LDAP object other than the default user **dn** object. For example, enter the mail object to check for an e-mail 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). **Note:** 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].
LDAP Filter	Enter an LDAP filter in this text box to perform a search using a filter criteria. The LDAP filter syntax is a logical expression in prefix notation meaning that logical operator appears before its arguments. For example, the item sn=Freddie means that the sn attribute must exist with the attribute value equal to Freddie. Multiple items can be included in the filter string by enclosing them in parentheses (such as sn=Freddie) and combined using logical operators such as the & (the ampersand conjunction operator) to create logical expressions. **Example:** The filter syntax (& (sn=Freddie) (mail=*)) requests LDAP entries that have both a sn attribute of Freddie and a mail attribute. More information about LDAP filter syntax can be found at http://www.ietf.org/rfc/rfc2254.txt and also at http://java.sun.com/products/jndi/tutorial/basics/directory/filter.html.

Oracle Database Monitor Settings

Description	The Oracle Database Monitor allows you to monitor the availability of an Oracle database server (versions 8i and 9i plus some earlier versions). The error and warning thresholds for the monitor can be set on one or more Oracle server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Oracle Database Monitor Overview" on page 479

The Oracle Database Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Database Connection URL	Enter the connection URL to the database you want to connect to. The syntax is jdbc:oracle:thin:@<server name or IP address>:<database server port>:<sid>. **Example:** To connect to the ORCL database on a machine using port 1521, use: jdbc:oracle:thin:@206.168.191.19:1521:ORCL. **Note:** The colon (:) and @ symbols must be included as shown.
Database Driver	Enter the driver used to connect to the database. **Example:** oracle.jdbc.driver.OracleDriver
Database User Name	Enter the user name that SiteScope should use to connect to the database. The specified user must be granted the permissions of a DBA.

GUI Element	Description
Database Password	Enter the password for the user name that SiteScope should use to connect to the database.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
DB Machine Name	Enter the name of the target database server.

Database Connection Settings

Description	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, dynamic updates, and database monitors (Oracle database, Database Counter, Database Query, DB2 8.x, Technology Database Integration, and so forth) can share and reuse database connections in a connection pool.

Important Information	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.
Useful Links	"JDBC Global Options" on page 232

The Database Connection Settings include the following elements:

GUI Element	Description
Use Connection Pool	If this check box is checked, SQL connection sharing is enabled. This means that you use a connection pool rather than open and close a new connection for each monitor query. This option is checked by default.
Physically Close if idle connection count exceeds	This is the maximum number of unused SQL connections in the SQL connection pool. When this number is exceeded, unused connections are closed rather than returned to the connection pool. **Default value:** 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. **Default value:** 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 feature. If your SQL driver does not support this feature, this parameter is ignored. **Default value:** 1 minute

SQL Server Monitor Settings

Description	The SQL Server Monitor allows you to monitor the availability and performance of an Microsoft SQL Server (versions 6.5, 7.1, 2000) on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more SQL Server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"SQL Server Monitor Overview" on page 481

The Add/Edit SQL Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the SQL Server you want to monitor is running. You cannot directly edit this field. Use the **Get Servers** button to enter a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see “Windows Remote Preferences Overview” on page 195 and “UNIX Remote Preferences Overview” on page 201.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Sybase Monitor Settings

Description	The Sybase Monitor allows you to monitor the availability and performance statistics of a Sybase Server. The error and warning thresholds for the monitor can be set on one or more Sybase server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Sybase Monitor Overview" on page 482

The Add/Edit Sybase Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Choose the server where the Sybase server you want to monitor is running. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.
User Name	Enter the user name to access the Sybase database.
Password	Enter the password of the user name to access the Sybase database.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

37

Generic Monitors User Interface Settings

This chapter includes the pages and dialog boxes that enable you to add and edit Generic monitors.

Composite Monitor Settings

Description	Designed to simplify the monitoring of complex network environments by checking the status readings of a set of other SiteScope monitors and/or monitor groups. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Composite Monitor Overview" on page 484

The Add/Edit ColdFusion Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Items	Choose one or more monitors (using CONTROL-CLICK) and/or groups that you want in the Composite Monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Monitor Delay	If **Run Monitors** is checked, this is the number of seconds to wait between running each monitor. This setting is useful if you need to wait for processing to occur on your systems before running the next monitor.
Run Monitors	Select if you want the Composite Monitor to control the scheduling of the selected monitors, as opposed to just checking their status readings. Monitors that are to be run this way should not also be run separately, so edit the individual monitors, set the **Update Every** 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.
Check All Monitors in Groups	When selected, all of the monitors in selected groups (and their subgroups) are checked and counted. **Default value:** A group is checked and counted as a single item when checking status readings.

Directory Monitor Settings

Description	The Directory Monitor watches an entire directory and reports on the total number of files in the directory, the total amount of disk space used, and the time (in minutes) since any file in the directory was modified. This information is useful if you have limited disk space, you want to monitor the number of files written to a specific directory, or you want to know the activity level in a certain directory. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Directory Monitor Overview" on page 485

The Add/Edit Directory Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	If the file is on a UNIX server, select the server name where the file is located. **Note:** Monitoring log files using SSH on Windows platforms is not supported for this monitor.

GUI Element	Description
Directory Path	Enter the directory that you want to monitor. ➤ **Remote Windows.** To monitor a directory on a remote machine in a Windows network, enter the UNC name for that directory. For example, \\server\directory\subdirectory. ➤ **Remote UNIX.** To monitor a directory on remote UNIX machines, the path must be relative to the home directory of the UNIX user account used to log in to the remote machine. You must also select the corresponding remote UNIX server in the Server field described above. For details on which UNIX user account to use for the applicable remote server, see "UNIX Remote Preferences Overview" on page 201. ➤ **Remote Windows NT/2000 server through NetBIOS.** You can also monitor directories on a remote Windows NT/2000 server through NetBIOS by including the UNC path to the remote directory. For example, \\remoteserver\sharedfolder\targetdirectory. 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 via the operating system is unsuccessful, SiteScope tries to match the \\remoteserver with servers currently defined as remote NT connection profiles (displayed in the Windows Remote Preferences servers list). If an exact match is found, SiteScope uses this connection profile to access the remote directory. 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 name of the directory. For details, see "SiteScope Date Variables" on page 1294.

Advanced Settings (Monitor Specific)

GUI Element	Description
No Subdirectories	Select this box if you do not want SiteScope to count subdirectories.
File Name Match	Enter text or an expression to match against (optional). Only file names which match are counted in the totals.

File Monitor Settings

Description	➤ Reads a specified file. ➤ Checks the size and age of a file. ➤ Helps you verify the contents of files by: ➤ Matching the contents for a piece of text, or by, ➤ Checking to see if the contents of the file have changed. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"File Monitor Overview" on page 486

The Add/Edit File Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	If the file is on a UNIX server, select the server name where the file is located. **Note:** Monitoring log files using SSH on Windows platforms is not supported for this monitor.
File Name	Enter the path and name to the file you want to monitor. For reading files on remote UNIX machines, the path must be relative to the home directory of the UNIX user account being used to login to the remote machine. **Example:** It may be necessary to provide the full path to the target file, such as /opt/application/logs/user.log. You must also select the corresponding remote UNIX server in the **Server** field described above. For details on which UNIX user account to use for the applicable remote server, see "UNIX Remote Preferences" on page 243. For reading files on remote Windows NT/2000 servers, you use NetBIOS to specify the server and UNC path to the remote log file. **Example:** \\remoteserver\sharedfolder\filename.log. You can also monitor files local to the server where SiteScope is running. **Example:** C:\application\appLogs\access.log. Optionally, you can use regular expressions for special date and time variables to match on log file names that include date and time information. **Example:** You can use a syntax of s/ex$shortYear$$0month$$0day$.log/ to match a current date-coded file. For details on using regular expressions and dates, see "SiteScope Date Variables" on page 1294.

GUI Element	Description
File Encoding	If the file content to be monitored uses an encoding that is different than the encoding used on server where SiteScope is running, enter the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the target file. This enables SiteScope to match and display the encoded file content correctly. **Examples:** Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.

Advanced Settings (Monitor Specific)

GUI Element	Description
Match Content	Enter a string of text to check for in the returned page. If the text is not contained in the page, the monitor displays **no match on content**. The search is case sensitive. HTML tags are part of a text document, so include them if they are part of the text you are searching for. This works for XML pages as well. **Example:** <B> Hello</B> World 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. **Example:** /href=Doc\d+\.html/ or /href=doc\d+\.html/i To save and display a particular piece of text as part of the status, use parentheses in a Perl regular expression. **Example:** /Temperature: (\d+). This returns the temperature as it appears on the page and this could be used when setting an Error if or Warning if threshold. For details, see “Using Regular Expressions” on page 1281. You can also use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression” on page 1397.

GUI Element	Description
Check for Content Changes	Unless this is set to "no content checking" (the default) SiteScope records a checksum of the document the first time the monitor runs and then does a checksum comparison each subsequent time it runs. If the checksum changes, the monitor has a status of "content changed error" and goes into error. If you want to check for content changes, you should use "compare to saved contents". The options for this setting are: ➤ **no content checking** (default). SiteScope does not check for content changes. ➤ **compare to last contents.** The new checksum is recorded as the default after the initial error **content changed error** occurs, so the monitor returns to OK until the checksum changes again. ➤ **compare to saved contents.** 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 **content changed error** and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents. ➤ **reset saved contents.** 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 **compare to saved contents** mode.
No Error if File Found	Check this if you want this monitor to remain in **GOOD** status, if the file is not found. The monitor status is **GOOD** regardless of how the monitor's thresholds have been configured.

JMX Monitor Settings

Description	Allows you to monitor the performance statistics of those Java-based applications that provide access to their statistics via the standard JMX remoting technology. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"JMX Monitor Overview" on page 487

The JMX Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
JMX URL	The URL to gather JMX statistics. Typically the URL begins with service:jmx:rmi:///jndi, followed by information specific to the application. For examples of URLs used for WebLogic and Tomcat, see "Creating a JMX Monitor for a WebLogic 9.x Server" on page 489.
Domain Filter	Domain filter to show only those counters existing within a specific domain (optional).
User Name	User name for connection to the JMX application (optional).
Password	Password for connection to the JMX application (optional).
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters. When the server being monitored is a WebLogic 9.x server, see "Creating a JMX Monitor for a WebLogic 9.x Server" on page 489 for further details.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Log File Monitor Settings

Description	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. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Log File Monitor Overview" on page 490

The Add/Edit Log File Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	If the log file is on a UNIX or NT SSH server, select the server name where the file located. The list of servers includes the remote UNIX or NT SSH servers that have been specified to SiteScope. **Note:** From SiteScope version 8.6, Remote Windows computers that use the NetBIOS connection method do appear in the **Servers** list. Use the UNC format to specify the path to the remote log file.

GUI Element	Description
Log File Pathname	Enter the pathname to the log file you want to monitor. ➤ For reading log files on remote UNIX machines, the path must be relative to the home directory of the UNIX user account being used to log in to the remote machine. You must also select the corresponding remote UNIX server in the Server field below. For information on which UNIX user account is being used for the applicable remote server, see "UNIX Remote Preferences Overview" on page 201. ➤ For reading log files on remote Windows NT/2000 servers using the NetBIOS method, use UNC to specify the path to the remote log file. **Example:** \\remoteserver\sharedfolder\filename.log ➤ For reading log files on remote Windows NT/2000 servers using the SSH method, specify the local path of the remote log file on the remote machine. **Example:** C:\Windows\System32\filename.log You must also select the corresponding remote Windows SSH server in the Servers field. For details on configuring a remote Windows server for SSH, see "Configuring Remote Windows Servers for SSH Monitoring" on page 1338. You can also monitor files local to the server where SiteScope is running. **Example:** C:\application\appLogs\access.log Optionally, you can use special date and time regular expression variables to match log file names that include date and time information. For example, you can use a syntax of s/ex$shortYear$$0month$$0day$.log/ to match a current date-coded log file. For details on using regular expressions, refer to "SiteScope Date Variables" on page 1294.

GUI Element	Description
Run Alerts	Select the method for running alerts for this monitor. ➤ If the **for each log entry matched** option is chosen, then the monitor triggers alerts for every matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error). ➤ If the **once, after all log entry have been checked** option is chosen, then the monitor counts up the number of matches and then triggers alerts. **Note:** 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.
Check from Beginning	Select the file checking option for this monitor instance. This setting controls what SiteScope looks for and how much of the target file is checked each time that the monitor is run. ➤ **Never.** Checks newly added records only. ➤ **First Time Only.** Checks the whole file once, and then newly added records only. ➤ **Always.** Always checks the whole file. **Default:** Never

GUI Element	Description
Content Match	Enter the text to look for in the log entries. You can also use a regular expression in this entry to match text patterns. Unlike the content match feature of other SiteScope monitors, the Log File Monitor content match is run repeatedly against the most recent content of the target log file until all matches are found. This means the monitor not only reports if the match was found but also how many times the matched pattern was found. To match text that includes more than one line of text, add an s search modifier to the end of the regular expression. For details, see "Using Regular Expressions" on page 1281. You can also use the Regular Expression Test tool to check your regular expressions. For details, see "Regular Expression" on page 1397. **Note:** If you enter more than four values in this box, when you generate a report by clicking the monitor title, the report includes only the first four values.

Advanced Settings (Monitor Specific)

GUI Element	Description
Rules File Pathname	In rare cases, it may be necessary to create a custom rules file to specify the log entries to match and the alerts to send. An example rules file is located in **<SiteScope root directory>/conf/examples/sample.rules**. Make a copy of this file and rename. There is no required naming convention. Open the file with the editor of your choice, and using the comments as a guideline, edit the file to meet your needs. When you are finished, type the full path name to your rules file in this field.
No Error if File Not Found	Select if you want this monitor to remain in GOOD status if the file is not found. The monitor status remains GOOD regardless of the monitor threshold configuration.
Match Value Labels	Use this option to enter labels for the matched values found in the target log file. The match value labels are used as variables to access retained values from the **Content Match** 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 **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. **Note:** If you enter more than four values in this box, when you generate a report by clicking the monitor title, the report includes only the first four values.

GUI Element	Description
Log File Encoding	If the log file content to be monitored uses an encoding that is different than the encoding used on server where SiteScope is running, enter the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the target log file. This enables SiteScope to match and display the encoded log file content correctly. **Examples:** Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.
Multi Line Match	Enables you to run a regular expression match on multiple lines of text.

Script Monitor Settings

Description	The Script Monitor runs an external command and reports the result. It is one way to integrate existing system management scripts into the SiteScope environment. The Script Monitor can be tailored to run scripts at regular intervals. In addition to reporting the command result, the Script Monitor can also parse and report a specific value from the command output. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Script Monitor Overview" on page 491

The Add/Edit Script Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	You can have SiteScope execute a script that is stored on a remote machine by: ➤ **Servers.** Select a server from the drop-down list. These are the remote servers that are available to SiteScope. **Note:** Only UNIX servers and Windows remote servers that use an SSH connection are listed. The Script monitor cannot use Windows remotes that do not use an SSH connection. ➤ **Other Server.** 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 the Remote UNIX Preferences page, enter the IP address or name of the server to monitor. **Default:** SiteScope executes script files that are stored locally on the SiteScope machine in the <**SiteScope install path**>/**SiteScope/scripts** directory.

GUI Element	Description
Script	Enter the name of the script to run. For security reasons, only scripts placed into the <**SiteScope install path**>/**SiteScope/scripts** directory may be used. In that directory, there are several examples scripts with comments describing each one. If you choose USE COMMAND, your must also specify a USE COMMAND script file name in the Advanced Settings section below. SiteScope sends the command or commands found in the USE COMMAND script file to be executed as a command line on the remote UNIX Machine. Script files for the USE COMMAND option must be created in the <**SiteScope install path**>/**SiteScope/scripts.remote** directory. **Example:** Create a file named **test.sh** and save it in the <**SiteScope install path**>/**SiteScope/scripts.remote** directory. Edit **test.sh** to include the command syntax ps -ef;echo "all done" as the content of the file. Then create a Script monitor with the USE COMMAND option selected, select a remote UNIX machine, and select test.sh as the USE COMMAND script to run. **Note:** The **diskSpace.bat** script only accepts two required parameters: host name and physical drive name. Since 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, it is recommended that you use the Disk Space monitor instead.

GUI Element	Description
Parameters	Use this text box to specify any additional parameters to pass to the script. Optionally, you can use a regular expression or one of SiteScope's date variables to insert date and time into the parameters box. **Example:** s/$month$ day $year$/ passes the current month, day and year to the script. **Field Exceptions:** For security reasons, the following characters are not allowed to be passed to scripts by SiteScope: ` (apostrophe), ; (semicolon), & (ampersand), | (vertical pipe), < (less than), > (greater than).

Advanced Settings (Monitor Specific)

GUI Element	Description
Match Value Labels	Enter labels for the matched values found in the script output. Separate multiple labels with a comma (,).
Remote Script Command File	If you have selected the USE COMMAND as the Script option above and a remote machine as the Server, select the script file that contains the commands that SiteScope should send to the remote machine. You can save one or more commands in the text script file and save the file in the <**SiteScope install path**>/**SiteScope/scripts.remote** directory. SiteScope opens this file and runs the command at the command line of the remote server chosen in the **Choose Server** option above. You can then use the Match Expression option to parse the output of the command and display valuable information. 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. You can use one or more commands per USE COMMAND script file. **Field Exception:** Do not include any carriage returns or any command that would normally discontinue script processing (for example, do not use the exit command).

GUI Element	Description
Cache Life	You use this option only if you want to use multiple Script monitor instances to check or match on content returned by a single run of a script. ➤ 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 executed again to update the cache and the monitor. ➤ Enter a value of **0** (zero) to disable the cache function. This causes the monitor to execute the script each time that it runs.
Match Expression	To retrieve a value from the script output, enter a regular expression in this box. **Example:** The expression: /(\d+)/ matches one or more digits returned by the script. 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. **Note:** If this item is left blank, no value is retrieved from the script.
Maximum For Measurement	(Optional) Enter a maximum value, in milliseconds, for creating the gauge display. **Example:** If the runtime of the script is 4 seconds, and this value is set to 8 seconds (8000 milliseconds), the gauge shows at 50%. **Default value:** 0

Web Service Monitor Settings

Description	The Web Service Monitor is used to check Simple Object Access Protocol (SOAP) enabled Web services for availability and stability. The Web Service Monitor sends a SOAP based request to the server and checks the response to verify that the service is responding. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Web Service Monitor Overview" on page 496

The Add/Edit Web Service Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Web Service Descriptor Language URL or WSDL File	Enter the URL of the WSDL file to be used for this monitor, and click the **Get Data** button. All file paths entered must be relative to the location **<SiteScope root directory>/SiteScope/templates.wsdl/** Your WSDL files must have the extension **.wsdl**. (Optional) Select a WSDL file from this drop-down list. This list reflects the files found by searching on **<SiteScope root directory>/SiteScope/templates. wsdl/*.wsdl**.
Get Data	Clicking the **Get Data** button causes the specified WSDL file to be retrieved and analyzed for method arguments. The ensuing page displays the measurements available for monitoring.

Advanced Settings (Monitor Specific)

GUI Element	Description
Content Match	Enter a string of text to check for in the returned page or frameset. If the text is not contained in the page, the monitor displays the message no match on content. 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. **Example:** "< B> Hello< /B> World" You may also perform a regular expression match by enclosing the string in forward slashes, with an i after the trailing slash to indicate that the search is not case-sensitive. **Example:** /href=Doc\d+\.html/ or /href=doc\d+\.html/i 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. **Example:** /Temperature: (\d+) **Note:** The search is case sensitive.
HTTP Content Type	The content type of the HTTP request.
HTTP User Agent	The HTTP user agent for the SOAP request.
Use .NET SOAP	Select this check box if the Web service is based on Microsoft .NET.
Request's Schema	The request schema. Currently SiteScope only supports SOAP.
Method Name Space	The XML name space for the method in the SOAP request. During initial setup, this value is extracted from the WSDL file.
Schema Name Space	The XML name space for the schema in the SOAP request. During initial setup, this value is extracted from the WSDL file.
SOAP ACTION	The SOAP ACTION URL in the header of the SOAP request to the Web Service. During initial setup, this is extracted from the WSDL file.

GUI Element	Description
NTLM Domain	If the Web service requires NTLM / Challenge Response authentication, a domain name is required as part of your credentials (as well as a user name and password below).
Authorization User Name	If the web service requires a user name and password for access (Basic, Digest, or NTLM authentication), enter the user name in this box. 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.
Authorization Password	If the web service requires a user name and password for access (Basic, Digest or NTLM authentication), enter the password in this box. 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.
Content Type	The SOAP http header content type value. **Default value:** text/xml; charset="utf-8"
HTTP Proxy	(Optional) A proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the URL, enter the name here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the URL, enter the password here. **Note:** Your proxy server must support Proxy-Authentication for these options to function.

XML Metrics Monitor Settings

Description	The XML Metrics Monitor allows you to monitor metrics for systems that make performance data available in the form of an XML file or page. The error and warning thresholds for the monitor can be set on one or more different objects. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"XML Metrics Monitor Overview" on page 499

The Add/Edit XML Metrics Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Authorization User Name	If the URL with the XML content you want to monitor requires a user name and password to access it, enter the user name in this box.
Password	If the URL with the XML content you want to monitor requires a name and password for access, enter the password in this box.
Proxy Server	(Optional) If you must use a proxy server to access the XML URL, enter the host or domain name and port of the proxy server in this box.

GUI Element	Description
Proxy Server User Name	If you use a proxy server and the proxy requires a name and password to access the target URL, enter the user name in this box. **Note:** The proxy server must support Proxy-Authenticate for these options to function.
XML URL	Enter the URL of the XML page or file that contains the metrics that you want to monitor.
XSL File	(Optional) Convert the XML metrics file into a format that SiteScope can use.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The number of seconds that the monitor should wait the XML page to complete downloading before timing-out. Once this time period passes, the monitor logs an error and reports an error status.
Authorization NTLM Domain	Enter the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL.
Preemptive Authorization	Select when the Authorization User Name and Authorization Password should be sent if SiteScope requests the target URL. ➤ **Use Global Preference.** Select to have SiteScope use the **When to Authenticate** setting as specified in the Preemptive Authorization section of the General Preferences page. ➤ **Authenticate first request.** Select to send the user name and password on the first request SiteScope makes for the target URL. **Note:** If the URL does not require a user name and password, this option may cause the URL to fail. ➤ **Authenticate if requested.** Select to send the user name and password on the second request if the server requests a user name and password. **Note:** If the URL does not require a user name and password, this option may be used. All options use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Default Authentication Username** and **Default Authentication Password** specified in the Main section of the General Preferences page are used, if they have been specified. **Note:** Preemptive Authorization does not control if the user name and password should be sent, or which user name and password should be sent.

GUI Element	Description
Accept Untrusted Certs for HTTPS	Check this option if you need to use certificates that are untrusted in the cert chain to access the target XML URL using Secure HTTP (HTTPS).
Accept Invalid Certs for HTTPS	Check this option if you need to accept an invalid certificate to access the target XML URL using Secure HTTP (HTTPS). This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.

38

Network Services Monitors User Interface Settings

This chapter includes the pages and dialog boxes that enable you to add and edit SiteScope monitors.

DHCP Monitor Settings

Description	Checks a DHCP Server via 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. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	➤ This monitor requires that a third-party Java DHCP library be installed on the server where SiteScope is running. The DHCP Monitor type does not appear in the interface until this library is installed. For more information, see "Installation of DHCP Software Library" on page 502. ➤ Monitors must be created in a group in the monitor tree.
Useful Links	"DHCP Monitor Overview" on page 502

The Add/Edit DHCP Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Timeout	Enter the time, in seconds, to wait for an IP address.

Advanced Settings (Monitor Specific)

GUI Element	Description
Requested Client Address	Optionally, the IP address to request from the DHCP server.

DNS Monitor Settings

Description	➤ Checks a Domain Name Server via the network. ➤ Verifies that the DNS server is accepting requests. ➤ Verifies that the address for a specific domain name can be found. Returns a status and writes it in the monitoring log file with each running. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"DNS Monitor Overview" on page 503

The Add/Edit DNS Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Host Name	Enter the host name to lookup. If you only want to verify that your DNS server is operating, the host name you enter here can be any valid host name or domain name. **Example:** 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 **Host address** box in the Advanced Settings section below.
DNS Server Address	Enter the IP address of the DNS server that you want to monitor. **Example:** 206.168.191.1

Advanced Settings (Monitor Specific)

GUI Element	Description
Host address	(Optional) You can use the DNS monitor to verify that a host name or domain name resolves to the correct IP address or addresses. Enter the IP address or addresses that are mapped to the **Host Name** (domain name) entered above. **Note:** If you enter more than one IP address, the monitor reports a status of good, even if only one of the IP addresses that you enter is mapped correctly to the **Host Name**. When using this option, the monitor only reports an error if none of the IP addresses entered in this field are mapped to the given **Host Name**.

FTP Monitor Settings

Description	Attempts to log into an FTP server and retrieve a specified file. A successful file retrieval indicates that your FTP server is functioning properly. Use this page to add a monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"FTP Monitor Overview" on page 504

The FTP Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
FTP Server	Enter the IP address or the name of the FTP server that you want to monitor. **Example:** 206.168.191.22 or ftp.thiscompany.com
File	Enter the file name to retrieve in this box. **Example:** /pub/docs/mydoc.txt
User Name	Enter the name used to log into the FTP server in this box. A common user name for general FTP access is user name anonymous.
Password	Enter the password used to log into the FTP server in this box. If using the anonymous login, the password is also anonymous.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The number of seconds that the FTP monitor should wait for a file to complete downloading before timing-out. Once this time period passes, the FTP monitor logs an error and reports an error status.
FTP Proxy	You may instruct SiteScope to run the FTP through a proxy server. Generally, if you use an FTP proxy you have it set up in your browser. Enter that same information here. Remember to include the port. **Example:** proxy.thiscompany.com:8080
Passive Mode	Select this box if you want SiteScope to use FTP passive mode. You use this mode to enable FTP to work through firewalls.
Proxy Server User Name	If the proxy server requires a name and password to access the file, enter the name here. The proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the file, enter the password here. The proxy server must support Proxy-Authenticate for these options to function.
Connection Timeout	The number of seconds that the FTP monitor should wait to connect to the FTP server before timing-out. Once this time period passes, the FTP monitor logs an error and reports an error status. **Default:** 30
Match Content	Enter a string of text to check for in the returned file. If the text is not contained in the file, the monitor displays **no match on content**. 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. **Example:** "/Size \d\d/" or "/size \d\d/i"

GUI Element	Description
Check for Content Changes	Use this option to have SiteScope compare file contents to a previous, successful download of a file. The options for this setting are: ➤ **no content checking** (default)**.** SiteScope does not check for content changes. ➤ **compare to last contents.** Any changed checksum is recorded as the default after the change is detected initially. Thereafter, the monitor returns to a status of **OK** until the checksum changes again. ➤ **compare to saved contents.** 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 content changed error and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents. ➤ **reset saved contents.** 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 **compare to saved contents** mode. For more information on checking for content changes, see “Check for Content Change” on page 505.

Formula Composite Monitor Settings

Description	Simplifies the monitoring of complex network environments by checking the status readings of two SNMP, Script, Database Query, or Windows Performance Counter monitors and performing an arithmetic calculation on their results. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Formula Composite Monitor Overview" on page 506

The Add/Edit Formula Composite Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Items	Choose two SNMP monitors, two Script monitors, two Database monitors, or two Windows Performance Counter monitors from the selection menu that the Formula Composite Monitor should operate on. You can select individual monitors and then click the right arrow to the right of the selection menu to move the monitor to the selection list on the right. Select the second monitor from the list on the left and click the right arrow to move the selection to the list on the right. You may also control-click two monitors on a single operation and click the right arrow to move them to the list on the right.
Operation	Select the arithmetic operation to be performed on the results of the two monitors selected above. For example: 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.

Advanced Settings (Monitor Specific)

GUI Element	Description
Run Monitors	Select this box if you want the Formula Composite Monitor to control the scheduling of the selected monitors, as opposed to just checking their status readings. This is useful if you want the monitors to run one after another or run at approximately the same time. **Note:** Any monitors that are to be run this way should not also be run separately, so edit the individual monitors, blank out the **Update Every** box for that monitor, and save the changes. Those monitors then only run when scheduled by the Formula Composite Monitor.
Monitor Delay	If Run Monitors is checked, this is the number of seconds to wait between running each monitor.
Constant	Enter an operator and a constant to operate on the result of the calculation specified in the **Operation** item above. For example, if an **Operation** of Add is selected above, entering the characters *8 in the **Constant** 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.
Result Label	Enter a name for the result of the formula calculation.

MAPI Monitor Settings

Description	The SiteScope MAPI Monitor checks a Messaging Application Program Interface (MAPI) server to confirm that e-mail operations can be executed. The SiteScope MAPI Monitor is designed to test the operation of a Microsoft Exchange Server. The error and warning thresholds for the monitor are set based on the e-mail delivery time. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"MAPI Monitor Overview" on page 508

The MAPI Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Receiver Server	Enter the hostname 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. It is recommended that you copy the server name as it appears in the Properties of the e-mail account you are using with this monitor.
Receiver Mailbox	Enter the name (alias) of the mailbox to be used for this monitor. This is often the e-mail account name but it may be a different name. It is recommended that you copy the mailbox name as it appears in the E-Mail Account properties for the e-mail account you are using with this monitor.

GUI Element	Description
Receiver Domain	Enter the domain to which both the owner of the mailbox being used and the Microsoft Exchange server belong. **Note:** 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.
Receiver User Name	Enter the NT account login name for the user associated with the above e-mail account.
Receiver User Password	Enter the NT account login password for the user name above.
Sender Server	Enter the sender's Microsoft Exchange server name. **Notes:** ➤ The MAPI sender is ignored if an SMTP sender is specified in the Advanced Settings. ➤ If no SMTP sender values are specified in the Advanced Settings, the receiver values are used if any of the sender values are not specified.
Sender Mailbox	Enter the alias of the sending mailbox.
Sender Domain	Enter the domain to which both the sending mailbox owner and the sending Microsoft Exchange server belong.
Sender User Name	Enter the login name for the NT account of the sending mailbox owner.
Sender Password	Enter the NT account login password for the sender account above.

Advanced Settings (Monitor Specific)

GUI Element	Description
Transaction Timeout	Enter the number of seconds for the monitor to wait for the message to arrive before the monitor should timeout. The monitor reports an error if timeout value is met before the e-mail message is delivered.
SMTP Server	Enter the SMTP server through which an outgoing message is sent. **Note:** If you set any of the SMTP values (**Server**, **Sender** or **Receiver**) they override the MAPI sender options specified in the Main Settings.
Sender	Enter the e-mail address of the SMTP sender.
Receiver	Enter the e-mail address of the receiver. This must match the receiver mailbox alias specified in the Main Settings
Attachment	Enter the full path name of a file to attach to the outgoing SMTP message.

Mail Monitor Settings

Description	The Mail Monitor checks a Mail Server via the network. It verifies 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 via 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. If SiteScope is unable to complete the entire loop, it generates an error message. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Mail Monitor Overview" on page 512

The Add/Edit Mail Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Action	Select the action the Mail Monitor should take with respect to the mail server: ➤ **Send and Receive.** This option allows 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. ➤ **Receive Only.** This option allows 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. **Note:** If the **Receive Only** option is selected, the Match Content text box must have a value to match against. Also note that if the **Receive Only** option is selected, you should use this monitor for a dedicated mail account that is NOT being accessed by any other mail client. If another mail client attempts to retrieve mail messages from the account that the Mail Monitor is monitoring in **Receive Only** mode, the monitor and the other mail client may lock each other out of the account such that neither is able to retrieve the messages. ➤ **Send Only.** This option checks that the receiving mail server has accepted the message.
Sending E-Mail Server (SMTP)	Enter the hostname of the SMTP mail server to which the test mail message should be sent. **Example:** mail.thiscompany.com
Send to Address	Enter the mail address to which the test message should be sent. This should be the address for the POP account that you specified in the Mail Server User Name box. **Example:** If you specified support as the Mail Server User Name, the To Address might be support@mycompany.com.

GUI Element	Description
Receiving Protocol	Select the protocol used by the receiving mail server. You use the POP3 option to check the POP3 mail server for a sent message. You use the IMAP4 option to check the IMAP mail server for a sent message.
Receiving E-Mail Server	Enter the hostname 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. **Example:** mail.thiscompany.com
Receiving E-Mail Server User Name	Enter a POP user account name on the receiving mail server. A test e-mail 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. **Example:** support **Note:** 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.
Receiving E-Mail Server Password	Enter a password, if necessary, for the receiving mail account.

Advanced Settings (Monitor Specific)

GUI Element	Description
RECEIVE ONLY Content Match	Enter a string of text to match against the contents of the incoming message. If the text is not contained in the incoming message, the monitor is in error. This is for the receiving only option. The search is case sensitive. **Example:** Subject:MySubject 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, < B> Hello< /B> World). This works for XML pages as well. 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. **Example:** /href=Doc\d+\.html/ or /href=doc\d+\.html/i If you want a particular piece of text to be saved and displayed as part of the status, use parentheses in a regular expression. **Example:** /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.
Timeout	The number of seconds that the Mail monitor should wait for a mail message to be received before timing-out. Once this time period passes, the Mail monitor logs an error and reports an error status.
POP Check Delay	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.

GUI Element	Description
Attachment	Enter the full path name of a file to add as an attachment to the e-mail message. Use this option to check that your e-mail 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. **Example:** s/C:\firstdir\$shortYear$$0month$$0day$/
Attachment Encoding	If the attachment file content uses an encoding that is different than the encoding used on server where SiteScope is running, enter the code page or encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the attachment file. **Examples:** Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.
SMTP User	Enter the user name required for SMTP authentication if the SMTP server requires authentication before sending messages.
SMTP Password	Enter the password for the SMTP authentication (if required).
NTLM Authentication	If NTLM authentication is used by the e-mail server, choose if you need version 1 or version 2.

Network Bandwidth Monitor Settings

Description	You use the Network Bandwidth Monitor to monitor SNMP-enabled network appliances such as routers and switches. The error and warning thresholds for the monitor can be set on one or more different objects. This monitor type also provides a Real-time metrics report, available as a link in the More column on the Group Detail Page. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Network Bandwidth Monitor Overview" on page 513

The Network Bandwidth Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Enter the name of the server you want to monitor.
SNMP Version	Select the version of SNMP to use when connecting.
Community	Enter the community string (valid only for version 1 or 2 connections).
SNMP V3 Authentication Type	Select the type of authentication to use for version 3 connections.
SNMP V3 Username	Enter the user name for version 3 connections.
SNMP V3 Authentication Password	Enter the authentication password to use for version 3 connections.
SNMP V3 Privacy Password	Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.
SNMP V3 Context Engine ID	Enter a hexadecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.

GUI Element	Description
SNMP V3 Context Name	Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.
Timeout	Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. **Default:** 5 seconds
Retries	Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. **Default:** 1
Port	Enter the port to use when requesting data from the SNMP agent. **Default:** 161
Starting OID	Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered in this field. You should edit this field only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value did not enable retrieving any counters, then you may have to enter a different value in this field. **Default:** 1
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box. Select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Device Type	Select an optional device type for device specific monitoring. The default is **Do not monitor device-specific metrics**. By specifying a device type, you enable the Network Bandwidth monitor to watch certain device-specific metrics. See the section entitled Device Specific Metrics Config File for more information on controlling the metrics associated with these device types and on adding new device types.
Duplex or Half-Duplex	Select the duplex state to use when calculating percent bandwidth utilized for all selected interfaces on this device.

GUI Element	Description
Interface index	Metrics for network interfaces on an SNMP-enabled device are presented as a table of management information (the ifTable), where each row corresponds to a different interface. Unfortunately, there is no requirement that the mapping 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: ➤ **Indexed by Interface Name.** The ifDescr field of the ifTable is used to maintain monitoring consistency across device reboots. ➤ **Indexed by Physical Address.** The ifPhysAddr field of the ifTable is used to maintain monitoring consistency across device reboots. ➤ **Indexed by ifTable Row Number.** SiteScope assumes that the interfaces remain in the same row in the ifTable across device reboots. **Note:** Some devices (Cisco, for instance) 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).
Show Bytes In/Out	Select this option to display a graph for bytes in/out along with the percent bandwidth utilized on the Real-Time Metrics page.
Real-Time Data Vertical Axis	Enter the maximum value on the vertical axis for real-time graphs (leave blank to have this automatically calculated by SiteScope)
Real-Time Data Time Window	Enter the number of hours for which real-time graph data should be stored.

Ping Monitor Settings

Description	The Ping Monitor checks the availability of a host via the network. Use this monitor to check that your connection to the Internet is available. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Ping Monitor Overview" on page 514

The Add/Edit Ping Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Host Name	Enter the IP address or the name of the host that you want to monitor. **Example:** 206.168.191.21 or demo.thiscompany.com

Advanced Settings (Monitor Specific)

GUI Element	Description
Time Out	The time, in milliseconds, that should pass before the ping times out. To change the threshold, type the new value in the text box. **Default value:** 5000 milliseconds
Packet Size	The size, in bytes, of the ping packets sent. To change the threshold, type the new value in the text box. **Default value:** 32 bytes

Port Monitor Settings

Description	The Port Monitor verifies that a connection can be made to a network port and measures the length of time it takes to make the connection. Optionally, it can look for a string of text to be returned or send a string of text once the connection is made. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Port Monitor Overview" on page 515

The Add/Edit Port Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Host Name	Enter the IP address or the name of the host that you want to monitor. **Example:** 206.168.191.21 or demo.thiscompany.com
Port Number	Choose the port number to connect to from the list of **Commonly Used Ports**, or enter a port number in the **Other Ports** text box. Additional entries can be added to the list by editing the **<SiteScope install path>/SiteScope/groups/master.config** file.

Advanced Settings (Monitor Specific)

GUI Element	Description
Send String	Customize the string sent to the host after a connection is made.
Match String	Check for a string of text after a connection is made. If the text is not received, the monitor displays the message no match on content. **Note:** The search is case sensitive.
Timeout	The number of seconds that the Port monitor should wait for the connection to the port, and for any sending and receiving to complete. Once this time period passes, the Port monitor logs an error and reports an error status.

RTSP Monitor Settings

Description	Real Time Streaming Protocol (RTSP) Monitor can be used to check the availability of certain kinds of time-based media files and real-time media streams. The RTSP Monitor does not support Real Media file types (for example, *.ra, *.ram files) or Windows Media files (for example, *.asf files). Use the Real Media Server Monitor and Real Media Player Monitor or the Windows Media Server Monitor and Windows Media Player Monitor ("Stream Monitors" on page 549) to monitor these types of services. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"RTSP Monitor Overview" on page 517

The Add/Edit RTSP Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Media URL	Enter the URL of the media file (for HTTP download and playback) or the URL of the media stream (for RTSP streaming) to be tested. **Note:** The RTSP Monitor may not process media reference files or media metadata files that are commonly used with RealNetworks RealPlayer reference files and with some QuickTime movies.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The time, in milliseconds, that should pass before the RTSP Monitor process is timed out. To change the threshold, type the new value in the text box. To test media files to completion, the Timeout value should be set to a value greater than the time that it should take to playback the subject media download. **Example:** If the media file should normally playback in 90 seconds, the Timeout value should be set for greater than 90 seconds. **Default value:** 60000 milliseconds
Stop Time	You can stop the media download after some specified amount of time has elapsed: ➤ A value of 0 causes the media stream to download until end of media is detected. ➤ A value greater than 0 stops the download of continuous broadcast streams (such as radio station multicasts) or very large media streams.
Maximum for Gauge Measurement	(Optional) Enter a maximum value for the Object ID. The maximum is calculated to create the gauge display.

SNMP Monitor Settings

Description	The SNMP Monitor reads a value from an SNMP device. Many network devices support the SNMP protocol as a way of monitoring them. You need to know the OIDs (Object ID's) for the device you want to monitor. These may be available in the product documentation or in the form of a MIB file. **Note:** To have SiteScope listen for SNMP traps from multiple devices, use the SNMP Monitor, "SNMP Monitor Overview" on page 521. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"SNMP Monitor Overview" on page 521

The Add/Edit SNMP Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Host Name	Enter the host name or IP address of the SNMP device that you want to monitor (for example, demo.thiscompany.com). **Default value:** 161 If your SNMP device is using a different port, add it to the hostname using **:port**. **Example:** demo.SiteScope.com:170 (to use port 170)

GUI Element	Description
Object ID	Select the Object ID mnemonic from the drop-down list or enter the Object Identifier (OID) for the SNMP value you want to retrieve. The OID specifies which value should be retrieved from the device. **Example:** 1.3.6.1.2.1.4.3 To troubleshooting basic connectivity to the device and to confirm that the SNMP agent is active, select the system.sysDescr object from the drop-down list if other objects can not be found. **Note:** SiteScope version 7.1 and later supports SNMP version 1 and version 2. To send a trap using snmpv2, you must select the version number in the Advanced Settings section. 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 need to provide an OID that is valid to the device to obtain a value. If you have a MIB file for the device you want to monitor, you can copy the *.mib (or *.my) file into the **<SiteScope install path>/SiteScope/templates.mib** 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** > **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. **Note:** 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).

GUI Element	Description
Index	The index of the SNMP object. Values for an OID come as either scalar or indexed (array or table) values. ➤ For a scalar OID, the index value must be set to 0. ➤ For an indexed or table value, you must provide the index (a positive integer) to the element that contains the value you want. For example, OID 1.3.6.1.2.1.2.2.1.17 is an indexed value that contains four elements. To access this second element of this OID you enter an index of 2 in the **Index** text box. To access the fourth element, enter an Index value of 4. In some vendor specific MIB's, the indexed entries (often referred to in tables) can have compound index values. For example, the OID for the process entry table in a Sun MicroSystems server MIB may be: .1.3.6.1.4.1.42.3.12.1.1. This indexed or table object may have up to eleven nodes with OIDs ranging from .1.3.6.1.4.1.42.3.12.1.1.1 to .1.3.6.1.4.1.42.3.12.1.1.11. Each of these nodes contains an indexed list of entries with index values that range from 0 to over 27300 where the Index value represents the process ID number used by the operating system (view examples using the ps -ef command in UNIX). In this example, the index values may not be consecutive from 0 to 27300.
Community	Enter the Community string for the SNMP device. The Community string provides a level of security for a SNMP device. Most devices use **public** as a community string. However, the device you are going to monitor may require a different Community string to access it. 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. **Note:** The field is valid only for version 1 or 2 connections.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	Enter the total number of seconds SiteScope should wait for a successful reply.
SNMP Version (V1, V2, or V3)	Select the SNMP version used by the SNMP host you want to monitor. SiteScope supports SNMP version 1, version 2, and version 3.
Retry Delay	Enter the number of seconds SiteScope should wait before retrying the request. It continues to retry at the interval specified here until the Timeout threshold is met. **Default value:** 1
Scaling	If you choose a scaling option from the **Commonly Used Values** 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 **Other Values** text box.
Match Content	Use this item to match against an SNMP value, using a string or a regular expression or XML names.
Units	Enter an optional units string to append when displaying the value of this counter.
Measurement Label	Enter an optional text string to describe the measurement being made by the monitor.
Measure as Delta	Click this box to have SiteScope report the measurement as the difference between the current value and the previous value.
Measure as Rate per Second	Click this box to have SiteScope divide the measurement by the number of seconds since the last measurement.
Percentage Base	Enter a number or SNMP object ID in this box. If entered, the measurement is divided by this value to calculate a percentage. If an object ID is entered, the Index value from the Main Settings pane is used.

GUI Element	Description
Measure Base As Delta	Select this option to have SiteScope calculate the Percentage Base as the difference between the current base and the previous base. Use this option when an SNMP object ID is used for Percentage Base and the object is not a fixed value.
Gauge Maximum	Enter a maximum value for the Object ID. The maximum is calculated to create the gauge display (Optional).
SNMP V3 Username	If you are using SNMP version 3, enter the user name to be used for authentication. **Note:** SiteScope only supports MD5 authentication for SNMP V3.
SNMP V3 Password	If you are using SNMP version 3, enter the password to be used for authentication for SNMP V3.

SNMP Trap Monitor Settings

Description	The SNMP Trap Monitor watches for SNMP Traps received by SiteScope from other devices. The agents for the SNMP enabled devices need to be configured to send traps to the SiteScope server. **Note:** To have SiteScope query a specific device for a specific value, use the SNMP Monitor, "SNMP Monitor Overview" on page 521. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.

Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"SNMP Trap Monitor Overview" on page 522

The Add/Edit SNMP Trap Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Run Alerts	Select the method for running alerts: ➤ If **For each SNMP Trap matched** is chosen, then the monitor triggers alerts for every matching entry found. ➤ If **Once, after all SNMP Traps have been checked** is chosen, then the monitor counts up the number of matches and triggers alerts based on the **Error if** and **Warning if** thresholds defined for the monitor in the Advanced Settings section.

GUI Element	Description
Content Match	Enter the text to look for in SNMP Traps. Regular expressions may also be used in this box for pattern matching. All SNMP Traps received by SiteScope are logged to **<SiteScope root directory>/logs/SNMPTrap.log** file. **Example:** The following shows two traps received from one router and another trap received from a second router: 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 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 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% 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.

Advanced Settings (Monitor Specific)

GUI Element	Description
Match Value Labels	Use this option to enter labels for the matched values found in the trap. The match value labels are used as variables to access retained values from the Content Match expression for use with the monitor threshold settings. 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. **Note:** Separate multiple labels with a comma (,).

SNMP by MIB Monitor Settings

Description	The SNMP by MIB Monitor allows you to monitor objects on any SNMP agent. The error and warning thresholds for the monitor can be set on one or more different objects. Use this page to add the monitor or edit the monitor’s properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“SNMP by MIB Monitor Overview” on page 523

The Add/Edit SNMP by MIB Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Enter the name of the server you want to monitor.
SNMP Version	Select the version of SNMP to use when connecting.
Community	Enter the community string. If you try to monitor SNMP agent through a specific community, you must make sure that the SNMP agent is familiar with that community. If you try to monitor Windows 2003 server through public community, you must make sure that the SNMP agent has this community configured. Otherwise, the monitor cannot connect to the agent. **Note:** This is valid only for version 1 or 2 connections.
SNMP V3 Authentication Type	Select the type of authentication to use for version 3 connections.
SNMP V3 Username	Enter the user name for version 3 connections.
SNMP V3 Authentication Password	Enter the authentication password to use for version 3 connections.
SNMP V3 Privacy Password	Enter the privacy password if DES privacy encryption is desired for version 3 connections. Leave blank if you do not want privacy.
SNMP V3 Context Engine ID	Enter a hexadecimal string representing the Context Engine ID to use for this connection. **Note:** This is applicable for SNMP V3 only.
SNMP V3 Context Name	Enter the Context Name to use for this connection. **Note:** This is applicable for SNMP V3 only.
Timeout	Enter the total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete.

GUI Element	Description
Retries	Enter the number of times each SNMP GET request should be retried before SiteScope considers the request to have failed.
Port	Enter the port to use when requesting data from the SNMP agent. **Default value:** 161
Starting OID	Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered in this field. **Default value:** 1 **Note:** You should edit this field 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 in this field.
MIB File	Select the MIB file which contains the objects you are interested in monitoring. If you select a specific MIB file, then only the objects described in that MIB file are displayed. If you select **All MIBs**, then all objects retrieved from the agent during the MIB traversal are displayed. If no MIB information is available for an object, it is still displayed but with no textual name or description. To make this monitor aware of new or additional MIBs, place new MIB files in the <**SiteScope root directory**>/**templates.mib** directory and restart SiteScope.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box. Select the counters you want to monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Counter Calculation Mode	Use this option to perform a calculation on objects of type Counter, Counter32, or Counter64. Calculations are either of the following: ➤ a simple delta of the current value from the previous value ➤ a rate calculation using the delta of current value from previous value, divided by the time elapsed between measurements **Note:** 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.

Windows Dial-up Monitor Settings

Description	The Windows Dial-up Monitor (available only on the Windows NT version of SiteScope) uses the Windows NT Remote Access Service to connect to an Internet Service Provider or Remote Access server and optionally runs a user-defined set of monitors. The monitor confirms that the dial-up connection can be established, and measures the performance of the connection and of the network services using the dial-up connection. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.

Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Windows Dial-up Monitor Overview" on page 526

The Add/Edit Windows Dial-up Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Phone Number	Type the phone number for the dial-up account, adding any extra modem digits or pauses that are required. **Example:** 9,4432266 includes a "9," for getting an outside line. Insert a comma wherever you need a short pause.
Account Login	The login name for the dial-up account.
Account Password	The password for the dial-up account.
Monitor(s) to Run	Select the groups and/or monitors that you want to run while the dial-up connection is established. Monitors that are used by Windows Dial-up Monitors should not be scheduled to run by themselves because some of their data would be via the dial-up connection, and some of their data would be through the local connection. Make sure that the **Update Every** box for these monitors is blank.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The timeout limits the total time that the Windows Dial-up Monitor takes to connect, authenticate, and run each of it is monitors. If the time ever exceeds this time, then the connection is hung up, and the monitor completes with a timeout error.

39

Server Monitors User Interface Settings

This chapter includes the pages and dialog boxes that enable you to add and edit SiteScope monitors.

Browsable Windows Performance Counter Monitor Settings

Description	The Browsable Windows Performance Counter Monitor tracks the values of Windows performance statistics. These are the same statistics that can be viewed using the Performance Monitor application under Windows. This monitor is only available on the Windows version of SiteScope. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	➤ This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ➤ This monitor can only be added by deploying a Solution template or SiteScope Health. For more information, see "Using SiteScope Templates" on page 1039 and "SiteScope Health Monitor Reference" on page 299. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. ➤ Monitors must be created in a group in the monitor tree.
Useful Links	"Browsable Windows Performance Counter Monitor Overview" on page 530

The Add/Edit Browsable Windows Performance Counter Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Choose the server where the performance counters you want to monitor are found. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.
Counter File	Choose the file that contains a list of counters from which to choose to monitor. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope. The files in this list all reside in the <**SiteScope install path**>**/SiteScope/templates.perfmon/browsable** directory under SiteScope. There are a number of default files in the standard SiteScope distribution.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

CPU Utilization Monitor Settings

Description	Reports the percentage of CPU time that is currently being used on the server. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"CPU Utilization Monitor Overview" on page 531

The Add/Edit CPU Utilization Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the CPU utilization you want to monitor is running. You cannot directly edit this field. Use the **Get Servers** button to enter or select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see “Windows Remote Preferences Overview” on page 195 and “UNIX Remote Preferences Overview” on page 201.

Disk Space Monitor Settings

Description	Track how much disk space is currently in use on your server. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Disk Space Monitor Overview" on page 532

The Add/Edit Disk Space Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the disk space you want to monitor is running. You cannot directly edit this field. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see "Configure SiteScope to Monitor a Remote Windows Server" on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.

GUI Element	Description
Disk	Select the disk drive that you want to monitor from the list. **Note:** Disk performance counters are disabled by default in standard Windows 2000 installations. In order for you to monitor disk drives using the SiteScope Disk Monitor on servers running Windows 2000, you must enable these disk counters. Use the diskperf -y command line on each Win2000 machine you want to monitor disk space and then reboot each server. You should then be able to select the disk drives for those servers in the SiteScope Disk Monitor form.

Exchange 2003 Mailbox Monitor Settings

Description	The Exchange 2003 Mailbox Monitor monitors mailbox statistics of Exchange Server 2003. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.

Important Information	➤ This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ➤ This monitor can only be added by deploying an Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information on using templates to deploy monitors, see "Using SiteScope Templates" on page 1039. ➤ Monitors must be created in a group in the monitor tree.
Useful Links	"Exchange 2003 Mailbox Monitor Overview" on page 533

The Add/Edit Exchange 2003 Mailbox Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Choose the server running Exchange Server 2003 that you want to monitor.
Username	Enter the user name to use when querying the server for mailbox statistics. The statistics are gathered via 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. **Default value:** If this field is left blank, the user that SiteScope is running is used.
Password	Enter the password for the user name entered above, or blank if user name is blank.

GUI Element	Description
N largest mailboxes	Enter the number (N) of mailboxes to display when reporting the N largest mailboxes.
Days since access	Enter the number of days (N) to use when reporting the number of mailboxes that have not been accessed in N days.

Advanced Settings (Monitor Specific)

GUI Element	Description
Reporting directory	Enter a location for SiteScope to save the results of each execution of this monitor. A default location is chosen if this field is left blank.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.

Exchange 2003 Public Folder Monitor Settings

Description	The Exchange 2003 Public Folder Monitor monitors public folder statistics of Exchange Server 2003. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	➤ This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ➤ This monitor can only be added by deploying an Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information on using templates to deploy monitors, see "Using SiteScope Templates" on page 1039. ➤ Monitors must be created in a group in the monitor tree.
Useful Links	"Exchange 2003 Public Folder Monitor Overview" on page 534

The Add/Edit Exchange 2003 Public Folder Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server	Choose the server running Exchange Server 2003 that you want to monitor.
Username	Enter the user name to use when querying the server for mailbox statistics. The statistics are gathered via 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. **Default value:** If this field is left blank, the user that SiteScope is running as is used.
Password	Enter the password for the user name entered above, or blank if user name is blank.
Days since access	Enter the number of days (N) to use when reporting the number of public folders that have not been accessed in N days.

Advanced Settings (Monitor Specific)

GUI Element	Description
Reporting directory	Enter a location for SiteScope to save the results of each execution of this monitor. **Default:** A default location is chosen if this field is left blank.
Timeout	The number of seconds that the monitor should wait for a response from the server before timing-out. Once this time period passes, the monitor logs an error and reports an error status.

Exchange 2000/2003 Message Traffic Monitor Settings

Description	The Exchange 2000/2003 Message Traffic Monitor monitors message statistics of Exchange Server 2000/2003. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	➤ This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ➤ This monitor can only be added by deploying an Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information on using templates to deploy monitors, see "Using SiteScope Templates" on page 1039. ➤ Monitors must be created in a group in the monitor tree.
Useful Links	"Exchange 2000/2003 Message Traffic Monitor Overview" on page 535

The Add/Edit Exchange 2000/2003 Message Traffic Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Recipient limit	Enter the number (N) of recipients to use when computing the number of messages sent to more than N recipients.
Log directory	The UNC path of the messaging tracking log file directory.
Query interval	Enter the number of minutes to look back for messages when computing statistics. This affects how long it takes to execute the monitor as a large interval could result in a large number of messages to be processed.
Number of outgoing users	Enter the number (N) of users to use for reporting the top N outgoing users.
Message size limit	Enter the number (N) of bytes to use when computing the number of messages sent larger than N bytes.
Number of domains	Enter the number (N) of domains to use for reporting the top N sending domains.

Advanced Settings (Monitor Specific)

GUI Element	Description
Reporting directory	Enter a location for SiteScope to save the results of each execution of this monitor. **Default:** A default location is chosen if this field is left blank.

Exchange 5.5 Message Traffic Monitor

Description	The Exchange 5.5 Message Traffic Monitor monitors message statistics of Exchange Server 5.5. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	➤ This monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP Sales representative for more information. ➤ This monitor can only be added by deploying an Exchange Solution template. Once the monitor has been created, you can edit the monitor configuration in the same way as other monitors. For information on using templates to deploy monitors, see "Using SiteScope Templates" on page 1039. ➤ Monitors must be created in a group in the monitor tree.
Useful Links	"Exchange 5.5 Message Traffic Monitor Overview" on page 536

The Add/Edit Exchange 5.5 Message Traffic Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Recipient limit	Enter the number (N) of recipients to use when computing the number of messages sent to more than N recipients.
Log directory	Enter a UNC path to the directory where message tracking logs are stored for the Exchange 5.5 server. Generally, this path is \\<server name>\tracking.log.
Query interval	Enter the number of minutes to look back for messages when computing statistics. This affects how long it takes to execute the monitor as a large interval could result in a large number of messages to be processed.
Number of outgoing users	Enter the number (N) of users to use for reporting the top N outgoing users.
Message size limit	Enter the number (N) of bytes to use when computing the number of messages sent larger than N bytes.
Number of domains	Enter the number (N) of domains to use for reporting the top N sending domains.

Advanced Settings (Monitor Specific)

GUI Element	Description
Reporting directory	Enter a location for SiteScope to save the results of each execution of this monitor. **Default:** A default location is chosen if this field is left blank.

IPMI Monitor Settings

Description	Monitors component health and operation statistics for Intelligent Platform Management Interface (IPMI) enabled devices running version 1.5. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"IPMI Monitor Overview" on page 537

The IPMI Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server Name	Enter the IPMI server name or IP address of the IPMI network adapter. **Note:** The IP address is normally not the same as the ordinary ethernet NIC adapter address.
Port Number	Enter the port number of the IPMI device. **Default:** 623
User Name	Enter the user name to access the IPMI server.
Password	Enter the password to access the IPMI server.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Memory Monitor Settings

Description	The Memory Monitor provides a tool for you to track how much virtual memory is currently in use on a server. Running out of memory can cause server applications to fail and excessive paging can have a drastic effect on performance. Use this page to add a monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Memory Monitor Overview" on page 538

The Memory Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the memory you want to monitor is running. You cannot directly edit this field. The default is to monitor memory on the server on which SiteScope is installed. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see "Configure SiteScope to Monitor a Remote Windows Server" on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.

Service Monitor Settings

Description	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. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Service Monitor Overview" on page 539

The Add/Edit Service Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the service you want to monitor is running. You cannot directly edit this field. The default is to monitor services on the server on which SiteScope is installed. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 218.

GUI Element	Description
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.
Service	Select the service (or process in UNIX) that you want to monitor from the **System Services** list. To monitor a service other than those listed, enter the name of the service in the **Other Service** box. To monitor an NT process, select **(Using Process Name)** in the drop-down list and enter the name in the **Process Name** text box (Advanced Settings pane). **Note:** The CPU % counter is relevant for processes and not for services, and it is displayed only if the selected service is by process name.

Advanced Settings (Monitor Specific)

GUI Element	Description
Process Name (NT Only)	If you want to get information about the percentage of CPU being used by a specific process and/or the number of a specific type of process running, enter the name of the process here. **Note:** The name of the process must be as it appears in NT Task Manager. **Example:** explorer.exe
Measure Process Memory Use (UNIX Only)	Select this box if you want SiteScope to report the amount of virtual memory being used by a specific process.

Threshold Settings (Monitor Specific)

GUI Element	Description
Error if/ Warning if/ Good if	The **CPU %** measurement is relevant only for processes and not for system services. If the selected service is a process name, **CPU %** measurement is in the drop-down list. If the selected service is a system service, such as Event Log, CPU % measurement is not listed.

UNIX Resources Monitor Settings

Description	The UNIX Resources Monitor enables you to monitor multiple system statistics on a single UNIX system. The error and warning thresholds for the monitor can be set on one or more server system statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"UNIX Resources Monitor Overview" on page 541

The Add/Edit UNIX Resources Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	Choose the server you want to monitor. Use the drop-down list to select a server from the list of remote servers that are available to SiteScope.
Get Measurements	Click to open the list of available measurements, and choose the server system measurements you want to check with the UNIX Resources Monitor. The Selected Measurements list displays the measurements currently selected for this monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Enable Server Centric Report	Select to enable collecting data specifically for generating the Server Centric Report. The report displays various measurements for the server being monitored. For details, see "Generating a Server Centric Report" on page 337.

Web Server Monitor Settings

Description	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. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Web Server Monitor Overview" on page 541

The Add/Edit Web Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Server (For SiteScope running on Windows)	The server where the Web Script instance you want to monitor is running. Enter the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. These are the remote servers that are available to SiteScope. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor.

GUI Element	Description
Web Server	Select a Web server type for the selected Web server from the list of accessible server types.
Log File Pathname (For SiteScope running on UNIX/Linux)	To monitor Web server statistics on UNIX servers, enter the full pathname of the Web server log file. Optionally, you can use a regular expression to insert date and time variables using SiteScope date variables. **Example:** s|/firstdir/$shortYear$$0month$$0day$| inserts SiteScope's date and time variables.

Advanced Settings (Monitor Specific)

GUI Element	Description
Log File Pathname	If your Web server does not appear in the Web Server list, you may still monitor it by entering the full path name to the Web server log file. **Example:** c:/ns-home/httpd-test/logs/access For servers that dynamically generate 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.
Request Size Column	If your Web server saves information in a custom format. Enter the column number which contains the Request Size. If this item is blank, the common log file format is assumed.

Windows Event Log Monitor Settings

Description	The Windows Event Log Monitor watches one of the Windows Event Logs (System, Application, or Security) for added entries. This monitor is only available on the Windows version of SiteScope. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Windows Event Log Monitor Overview" on page 542

The Add/Edit Windows Event Log Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the event log you want to monitor is running. You cannot directly edit this field. The default is to monitor the server on which SiteScope is installed. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see "Configure SiteScope to Monitor a Remote Windows Server" on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.

GUI Element	Description
Log Name	Choose from the following logs: ➤ System ➤ Application ➤ Security ➤ Directory Service ➤ DNS ➤ File Replication Service **Note:** This is a static list of those logs available when deploying this monitor. These log files do not necessarily exist on the server you are monitoring.
Event Type	Select the event type: ➤ Any ➤ Error ➤ Warning ➤ Error or Warning ➤ Information
Run Alert	Select the method for running alerts. If **for each event matched** is chosen, then the monitor triggers alerts for every matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error). If **once, after all events have been checked** is chosen, then the monitor counts up the number of matches and triggers alerts.

Advanced Settings (Monitor Specific)

GUI Element	Description
Source and ID Match	Enter the match string identifying the source of the event and the event ID in the form: <Event Source>:<Event ID>. **Example:** Enter Print:20 to match event source named Print and event ID of 20. To match against all events from a specific source, enter just the event source name. **Example:** W3SVC To match an exact event ID from an event source, specify both. **Example:** Service Control Mar:7000 You can also use a regular expression for more complex matches. You can also use the Regular Expression Test tool to check your regular expressions. For details, see "Regular Expression" on page 1397.

GUI Element	Description
Source and ID NOT Match	Enter the match string identifying the source of the event to NOT MATCH in the form: <Event Source>:<Event ID>. **Example:** Print:20 ignores all events of Print source and event ID 20. To ignore all events from a particular source, specify just the source name. **Example:** W3SVC To ignore an exact event ID from an event source, specify both. **Example:** Service Control Mar:7000 You can also use a regular expression for a more complex NOT MATCH. **Example:** ➤ to ignore all Perflib sources from 200 to 299 use: /Perflib:2\d\d/ ➤ to ignore all events from the Perflib source, use: Perflib:* You can also use the Regular Expression Test tool to check your regular expressions. For details, see "Regular Expression" on page 1397.
Description Match	Enter the text string to match against the description text for the event entry. 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. You can also enter a regular expression in this field to match on patterns. You can also use the Regular Expression Test tool to check your regular expressions.

GUI Element	Description
Description Not Match	Windows Event Log Monitor triggers an alert only if the text entered in this box does not appear in the event entry's description text. The description text can be viewed in the detail view of the event log entry via the Windows Event Viewer. You can also enter a regular expression in this field to match on patterns. You can also use the Regular Expression Test tool to check your regular expressions. For details, see “Regular Expression” on page 1397.
Event Category	Match the category number of the event entry.
Event Machine	Match against the machine that added the entry to the log file.
Interval	Enter an time period, in minutes, 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. **Example:** 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** >= **3**.

Windows Performance Counter Monitor Settings

Description	The Windows Performance Counter Monitor tracks the values of any Windows performance statistic. These are the same statistics that can be viewed using the Performance Monitor application under Windows. This monitor is only available on the Windows version of SiteScope. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Windows Performance Counter Monitor Overview" on page 543

The Add/Edit Windows Performance Counter Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server on which you want to monitor Windows performance statistics. You cannot directly edit this field. The default is to monitor the server on which SiteScope is installed. Use the **Get Servers** button to select a server name. When using a settings file from the Windows Performance Counter Monitor, all counters are measured on the server specified by this entry.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 218.

GUI Element	Description
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see “Windows Remote Preferences Overview” on page 195 and “UNIX Remote Preferences Overview” on page 201.
Perfmon Chart File	Select the Windows Performance Counter Monitor setting file you want to use for your settings. These files can be saved in the Windows Performance Counter Monitor (perfmon) and have either a .pmc or .pmw extension. On Windows 2000 Platform these can be saved using the .htm format. The files in this list all reside in the **<SiteScope install path>/SiteScope/templates.perfmon** directory under SiteScope. There are a number of default files in the standard SiteScope distribution. **Note:** If you make your own settings file, it must be placed in the **<SiteScope install path>/SiteScope/templates.perfmon** directory. You can optionally specify the settings directly for a single counter below under the Advanced Settings section. If you create your own .pmc file, any server specified in the .pmc file is ignored by SiteScope. The server to be queried is the one selected via the **Server** selection box on monitor setup page (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 Windows Performance Counter Monitor instance, but any single instance of the Windows Performance Counter Monitor only queries one server regardless of the servers assigned in the .pmc. If you have specified the settings directly in the Advanced Settings section, this list displays **(Custom Object)**.

Advanced Settings (Monitor Specific)

GUI Element	Description
Object	The Object is the same as the "Object" in the Performance Monitor application - just type it in this box. The Object is the high level item that is measured, such as Processor or Server. The object name is case sensitive. If you are using a Performance Monitor file for counter settings, leave this item blank.

Counter	The counter is the same as the "Counter" in the Performance Monitor application - just type it in this box. The Counter is the specific aspect of the Object that is measured, such as Interrupts/sec. The counter name is case sensitive. If you are using a Performance Monitor file for counter settings, leave this item blank.
	Some examples of Objects and Counters available to the Windows Performance Counter Monitor include:
	➤ System
	  ➤ % Total Processor Time
	  ➤ File Data Operations/sec
	  ➤ Processor Queue Length
	  ➤ Total Interrupts/sec
	➤ Processor
	  ➤ % Processor Time
	➤ Objects
	  ➤ Threads
	➤ Process
	  ➤ Private Bytes
	➤ Physical Disk
	  ➤ % Disk Time
	➤ Memory
	  ➤ Page Faults/sec
	  ➤ Pages/sec
	  ➤ Pool Nonpaged Bytes

GUI Element	Description
Instance	Some counters can have multiple instances - for example, on machines with two CPUs, there are two instances of the Processor object. The instance is the same as the "Instance" in the Performance Monitor application - just type it in this box. Note that the instance name is case sensitive. If you are using a Performance Monitor file for counter settings, leave this item blank.
Units	If you want units to be displayed with the counter's values to make them more readable, enter the units here.
Scale	If you want the raw performance counter value scaled to make it more readable, select the scale here. 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 via a Performance Monitor file, this scaling applies to all counters.
Baseline Interval	Enter the number of monitor runs to be averaged for use as a Rolling Baseline. Rolling baselines are calculated for an interval equal to time to complete the number of monitor runs entered here. For more information, see Setting up and Using Rolling Baselines. For details, see “Set Monitor Thresholds Using a Rolling Baseline” on page 405.

Windows Resources Monitor Settings

Description	The Windows Resources Monitor allows you to monitor system performance data using the Performance Data Helper (PDH) interface on Windows systems. The error and warning thresholds for the monitor can be set on one or more performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Windows Resources Monitor Overview" on page 544

The Add/Edit Windows Resources Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the Windows Resources Monitor you want to monitor is running. You cannot directly edit this field. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 218.

GUI Element	Description
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.
Get Measurements	Click to open the list of available measurements, and select the objects, instances, and counters you want to check with the Windows Resources Monitor. The performance parameters or counters available for the Windows Resources Monitor vary depending on what operating system options and applications are running on the remote server. The Selected Measurements list displays the measurements currently selected for this monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Collection Method	Select the collection method from the following options: ➤ **Windows PDH Library**. This is the default and most common option. ➤ **Use Global Setting**. Instructs the monitor to use the value configured in the **master.config** file for the **_wrmCollectionMethod** property. If this property has not been added to the **master.config** file, the default option is used. ➤ **Direct Registry Queries**. 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.
Enable Server Centric Report	Select to enable collecting data specifically for generating the Server Centric Report. The report displays various measurements for the server being monitored. For details, see "Generating a Server Centric Report" on page 337.

Windows Services State Monitor Settings

Description	The Windows Services State Monitor is used to monitor a list of services running on Windows systems and report changes in the number of services that are running and list the services that changed state. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Windows Services State Monitor Overview" on page 548

The Add/Edit Windows Services State Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server you want to monitor. You cannot directly edit this field. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see “Windows Remote Preferences Overview” on page 195 and “UNIX Remote Preferences Overview” on page 201.

Advanced Settings (Monitor Specific)

GUI Element	Description
Services to Include	Enter an optional regular expression to filter the list of services returned by the monitor. **Default:** all of the services detected on the remote machine. 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. Examples of services which can be monitored are: ➤ 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
Services to Ignore	Enter an 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.
Include Driver Services	Select this box to have the monitor include all low-level driver services. 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.

40

Stream Monitors User Interface Settings

This chapter includes the pages and dialog boxes that enable you to add and edit SiteScope monitors.

Real Media Player Monitor Settings

Description	The Real Media Player Monitor allows you to emulate a user playing media or streaming data from a Real Media Server. The error and warning thresholds for the monitor can be set on one or more Real Media Player performance statistics. This monitor does not support metadata files such as the .smi format. Use this page to add the monitor or edit the monitor’s properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“Real Media Player Monitor Overview” on page 549

The Add/Edit Real Media Player Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Counters	Choose the server performance counters you want to check with this monitor. The list to the right of this item displays the available counters and those currently selected for this monitor.
URL	Enter the URL of the media file or streaming source you want to monitor. This should be the URL of the media file. **Note:** ➤ Only monitor video, not audio, streams with this monitor. ➤ This monitor does not support metadata files such as the .smi format.

Advanced Settings (Monitor Specific)

GUI Element	Description
Duration	Enter the playback duration (in milliseconds) that the monitor should use for the media file or source indicated by the **URL** above. The duration value does not need to match the duration of the media contained in the file. **Example:** You can direct SiteScope to monitor a media file that contains 45 seconds of media content. The default **Duration** for the Real Media Player Monitor is 15000 milliseconds which equals 15 seconds. In this configuration, the monitor instance would connect to the media source and play the media content for 15 seconds and report the status for those 15 seconds. 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.

Real Media Server Monitor Settings

Description	The Real Media Server Monitor allows you to monitor the availability of an Real Media Server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more Real Media Server performance statistics. Use this page to add a monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Real Media Server Monitor Overview" on page 550

The Add/Edit Real Media Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the Real Media Server you want to monitor is running. You cannot directly edit this field. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see “Configure SiteScope to Monitor a Remote Windows Server” on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see “Windows Remote Preferences Overview” on page 195 and “UNIX Remote Preferences Overview” on page 201.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

Windows Media Player Monitor Settings

Description	The Windows Media Player Monitor allows you to emulate a user playing media or streaming data from a Windows Media Server. The error and warning thresholds for the monitor can be set on one or more Windows Media Player performance statistics. This monitor does not support the .asx or .mov formats. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Windows Media Player Monitor Overview" on page 551

The Add/Edit Windows Media Player Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
URL	Enter the URL of the media file or streaming source you want to monitor. This should be the URL of the media file. **Example:** mms://<servername>/sample.asf for a unicast stream or http://<servername>/stationid.nsc for a multicast stream using a Windows Media Server multicast station program. **Note:** This monitor does not support the .asx or .mov formats.

GUI Element	Description
Counters	Select the media player performance parameters or counters you want to check with the Windows Media Player Monitor. For details of the available parameters or counters, see "Performance Counters" on page 551.

Advanced Settings (Monitor Specific)

GUI Element	Description
Duration	Enter the playback duration, in milliseconds, that the monitor should use for the media file or source indicated by the **URL** above. The duration value does not need to match the duration of the media contained in the file. **Default value:** 15000 milliseconds (15 seconds) **Example:** If a media file contains 45 seconds of media content, and you use the default setting of 15 seconds, the monitor instance connects to the media source and plays the media content for 15 seconds and reports the status for those 15 seconds. 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.

Windows Media Server Monitor Settings

Description	The Windows Media Server Monitor allows you to monitor the availability of a Microsoft Windows Media server on Windows NT systems. The error and warning thresholds for the monitor can be set on one or more Windows Media server performance statistics. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Windows Media Server Monitor Overview" on page 553

The Add/Edit Windows Media Server Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Servers	The server where the Windows Media Server you want to monitor is running. You cannot directly edit this field. Use the **Get Servers** button to select a server name.
Get Servers	Click to open the Server List dialog box. Select the server you want to monitor by: ➤ **Servers.** Select a server from the drop-down list. The list displays the servers visible in the local domain and the servers configured in Remote Preferences. ➤ **Other Server.** 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 Preferences, enter the IP address or name of the server to monitor. **Note:** To monitor a remote server, you must have domain privileges or authenticated access to the remote server. For details, see "Configure SiteScope to Monitor a Remote Windows Server" on page 218.
Display only configured servers	Select to limit the list of servers that appears in the Server List dialog box to only those servers that have been configured in Windows/UNIX Remote Preferences. For details, see "Windows Remote Preferences Overview" on page 195 and "UNIX Remote Preferences Overview" on page 201.
Counters	The server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Click to open the Get Counters dialog box, and select the counters you want to monitor.

41

Web Transaction Monitors User Interface Settings

This chapter includes the pages and dialog boxes that enable you to add and edit SiteScope monitors.

eBusiness Transaction Monitor Settings

Description	Verifies that the multiple tasks that make up an online transaction are completed properly. This includes: ➤ Successful navigation through a series of URLs ➤ Transmission of an e-mail confirming the sequence. ➤ Logging the information into a database file. Runs a sequence of other SiteScope monitors, checking that each monitor returns a status of OK. Reports an Error status if any monitor in the sequence fails. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"eBusiness Transaction Monitor Overview" on page 555

The Add/Edit eBusiness Transaction Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Items	Using the control key or equivalent, click the group or set of monitors that make up the eBusiness Transaction Monitor. As noted in the set up section above, the monitors are run in the order that they are listed in their group.

Advanced Settings (Monitor Specific)

GUI Element	Description
Monitor Delay	Enter a number of seconds to wait between running each monitor. This setting is useful if you need to wait for processing to occur on your systems before running the next monitor.
When Error	Choose how you want errors during the sequence to be handled: ➤ **Continue, run the remainder of the monitors.** This runs every monitor no matter what the status of a given monitor is. ➤ **Stop, do not run any of the remaining monitors.** This stops running the list of monitors immediately, if a monitor returns an error. ➤ **Run the last monitor.** 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.
Single Session	Select this box if you want any URL monitors to use the same network connection and the same set of cookies. This is useful if you are using the eBusiness Transaction Monitor to group several URL Sequence monitors and do not want to include the login steps as part of each transaction.

Link Check Monitor Settings

Description	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. Use this page to add the monitor or edit the monitor’s properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	“Link Check Monitor Overview” on page 558

The Link Check Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
URL	Enter the URL that is the starting point for checking links. The link monitor retrieves the page for this URL. Next, it 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. **Example:** http://demo.thiscompany.com
Search External Links	Select this option to have the Link Check Monitor follow all links on each page and not just links that contain the original base URL. **Warning:** 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 **Maximum Links** setting and limit the depth of the search using the **Maximum Hops** setting in the Advanced Settings.

GUI Element	Description
Maximum Links	The maximum number of links this monitors checks. When the maximum number of links is reached the monitor stops and reports the results of those links that were checked. Increase this number if you have a large site and want to check every link on the site.
Maximum Hops	The maximum number of internal links that SiteScope should follow from the starting URL. Limiting the number of links reduces the number of URLs that SiteScope follows and shortens the time to complete the report. SiteScope does not follow any links on external pages. Select one of the predefined choices using the **Commonly Used Values** list. To enter your own limit, enter a numeric value in the **Other Values** box. **Example:** 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.

Advanced Settings (Monitor Specific)

GUI Element	Description
Pause	The delay, in milliseconds, between each link check. Larger numbers lengthen the total time to check links but decrease the load on the server.
Timeout	The number of seconds that the URL monitor should wait for a page to begin downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status.
Authorization User Name	If the URL specified requires a user name for access, enter the name in this box.
Authorization Password	If the URL specified requires a password for access, enter the password in this box.
HTTP Proxy	Optionally, a proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name to access the URL, enter the name here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a password to access the URL, enter the password here. Technical note: your proxy server must support Proxy-Authenticate for these options to function.
Post Data	Enter any form values required for the first page being checked. This is useful if you need to log in via an HTML form to reach the rest of the site that you are checking.

URL Monitor Settings

Description	The URL Monitor is one of the most versatile and powerful Web monitoring tools available to Webmasters and system administrators. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"URL Monitor Overview" on page 559

The Add/Edit URL Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
URL	Enter the URL that you want to monitor. **Example:** http://demo.thiscompany.com 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. **Example:** https://www.thiscompany.com
Match Content	Enter a string of text to check for in the returned page or frameset. If the text is not contained in the page, the monitor displays the message content match error. 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. **Example:** < B> Hello< /B> World You can also perform a regular expression match by enclosing the string in forward slashes, with a letter i after the trailing slash indicating case-insensitive matching. **Example:** /href=Doc\d+\.html/ or /href=doc\d+\.html/i 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. **Example:** /Temperature: (\d+). This returns the temperature as it appears on the page and this could be used when setting an **Error if** or **Warning if** threshold. **Note:** The search is case sensitive.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The number of seconds that the URL monitor should wait for a page to complete downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status. If you have checked the Retrieve Frames or Retrieve Images option, SiteScope waits for these items to be retrieved before considering the page to be fully downloaded.
Retrieve Images	Select this box if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by IMG, BODY (from the background property), and INPUT TYPE=IMAGE HTML tags. Images that appear more than once in a page are retrieved only once. **Note:** If this option is checked, each image referenced by the target URL contributes to the download time. However, if a image times out during the download process or has a problem during the download, that time is not added to the total download time.
Retrieve Frames	Select this box if you want SiteScope to retrieve the frames references in a frameset and count their retrieval time in the total time to download this page. Frames include those referenced by FRAME and IFRAME tags. If **Retrieve Images** is also checked, SiteScope attempts to retrieve all images in all frames. **Note:** 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.

GUI Element	Description
Use WinInet	Select this option if you want to use WinInet as an alternative HTTP client for this monitor. **Default value:** Apache Select this option to use WinInet instead of Apache when: ➤ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates while Apache does not. ➤ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.
Error If Match	Enter a string of text to check for in the returned page or frameset. If the text is contained in the page, the monitor indicates an error condition. HTML tags are part of a text document, so include them if they are part of the text for which you are searching. **Example:**< B> Error < /B> Message 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. **Example:** /href=Doc\d+\.html/ or /href=doc\d+\.html/i **Note:** The search is case sensitive.

GUI Element	Description
Check for Content Changes	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 go into error. If you want to check for content changes, you usually want to use **compare to saved contents**. The options for this setting are: ➤ **no content checking** (default). SiteScope does not check for content changes. ➤ **compare to last contents.** The new checksum is recorded as the default after the initial error **content changed error** occurs, so the monitor returns to OK until the checksum changes again. ➤ **compare to saved contents.** 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 **content changed error** and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents. ➤ **reset saved contents.** 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 **compare to saved contents** mode. **Default value:** no content checking
Baseline Interval	Enter the number of monitor runs to be averaged for use as a rolling baseline. Rolling baselines are calculated for an interval equal to the time to complete the number of monitor runs entered here. For details, see "Set Monitor Thresholds Using a Rolling Baseline" on page 405.

GUI Element	Description
HTTP Version	Select this box to force SiteScope to use HTTP version 1.0 style request headers. When unselected, SiteScope uses HTTP Version 1.1 in the request header to the target server. **Default value:** HTTP 1.1
Retries	Enter the number of times that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request for is a recoverable error.
Accept Untrusted Certs 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 SSL Connectivity in "URL Monitor Overview" on page 559.
Accept Invalid Certs for HTTPS	Check 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.
When to Encode Post Data	Determines if the Post Data is encoded. Select from the following options: ➤ **Use content type.** Decide to encode the post data by the content type header. If the header equals urlencoded then encode, otherwise do not encode. ➤ **Force URL encoding.** Always encode the post data. ➤ **Force NO URL encoding.** Do not encode the post data.
Authorization User Name	If the URL specified requires a name and password for access, enter the user name in this box. Alternatively, you can leave this entry blank and enter the user name in the Default Authentication Credentials section on the General Preferences page. Use this alternate method to define common authentication credentials for use with multiple monitors.

GUI Element	Description
Authorization Password	If the URL specified requires a name and password for access, enter the password in this box. Alternatively, 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 monitors.
Authorization NTLM Domain	Enter the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL.
NTLM V2	Select this option if the URL you are accessing requires authentication using NTLM version 2.

GUI Element	Description
Preemptive Authorization	Select when the Authorization User Name and Authorization Password should be sent if SiteScope requests the target URL. ➤ **Use Global Preference.** Select to have SiteScope use the **When to Authenticate** setting as specified in the Preemptive Authorization section of the General Preferences page. ➤ **Authenticate first request.** Select to send the user name and password on the first request SiteScope makes for the target URL. **Note:** If the URL does not require a user name and password, this option may cause the URL to fail. ➤ **Authenticate if requested.** Select to send the user name and password on the second request if the server requests a user name and password. **Note:** If the URL does not require a user name and password, this option may be used. All options use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Default Authentication Username** and **Default Authentication Password** specified in the Main section of the General Preferences page are used, if they have been specified. **Note:** Preemptive Authorization does not control if the user name and password should be sent, or which user name and password should be sent.
HTTP Proxy	(Optional) A proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the URL, enter the name here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.

GUI Element	Description
Proxy Server Password	If the proxy server requires a name and password to access the URL, enter the password here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Proxy NTLM V2	Select this option if the proxy requires authentication using NTLM version 2.
Client Side Cert	If you need to use a client side certificate to access the target URL, select the certificate file using the drop down menu. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You enter the password for the certificate in the **Client Side Cert Password** field. **Note:** Client side certificate files must be copied into the <SiteScope root directory>/templates.certificates directory.
Client Side Cert Password	If you are using a client side certificate and that certificate requires a password, enter the password in this field.

GUI Element	Description
Post Data	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. See also the Match Content item for a way to verify that the correct form response was received. If this item is blank, a GET request is performed. The POST Data can be used to send cookie data. To send cookies with the request, use the format Set-cookie: cookieName=cookieValue. To change the content type of a post, use the format Content-Type: application/my-format. To hide values in the POST data, add a line like: _private=_name=mysecret _value=rosebud _private=_name=mypassword _privateValue=sesame and then use the following form in the POST Data: s|username=$private-mysecret$| s|password=$private-mypassword$| and SiteScope substitutes the values from the **master.config** into the POST Data.
URL Content Encoding	SiteScope retrieves the correct encoding from the server response. The default value appearing in this field should not be edited. **Examples:** Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.

GUI Element	Description
Error If Redirected	Select this box if you want SiteScope to notify you if a URL is redirected. **Default:** SiteScope follows redirects without reporting an error.
Show Detailed Measurement	Select this box if you want SiteScope to record a detailed break down of the process times involved in retrieving the requested URL. These measurements include the following: ➤ **DNS lookup time.** The time it takes to send a name resolution request to your DNS server until you get a reply. ➤ **Connection time.** The time it takes to establish a TCP/IP/Socket connection to the Web server. ➤ **Server response time.** The time after the request is sent until the first byte (rather first buffer full) of the page comes back. ➤ **Download time.** The time it takes to download the entire page.

URL Content Monitor Settings

Description	The URL Content Monitor is a specialized variation of the URL Content Monitor Overview 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. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"URL Content Monitor Overview" on page 563

The Add/Edit URL Content Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
URL	Enter the URL that you want to monitor. **Example:** http://demo.thiscompany.com If you are monitoring a secure URL, the URL must reflect the correct transfer protocol. **Example:** https://demo.thiscompany.com
Match Content	Enter an expression describing the values to match in the returned page. If the expression is not contained in the page, the monitor displays the message no match on content. A regular expression is used to define the values to match. **Example:** The expression /Copyright (\d*)-(\d*)/ would match two values, 1996 and 1998, from a page that contained the string Copyright 1996-1998. The returned value could be used when setting an Error if or Warning if thresholds.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The number of seconds that the URL monitor should wait for a page to begin downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status.
Retrieve Images	Select this box if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by 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. **Note:** 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.
Retrieve Frames	Select this box if you want SiteScope to retrieve the frames references in a frameset and count their retrieval time in the total time to download this page. Frames include those referenced by FRAME and IFRAME tags. If **Retrieve Images** is also checked, SiteScope attempts to retrieve all images in all frames. **Note:** If the **Retrieve Frames** 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.

GUI Element	Description
Use WinInet	Select this option if you want to use WinInet as an alternative HTTP client for this monitor. **Default value:** Apache Select this option to use WinInet instead of Apache when: ➤ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates while Apache does not. ➤ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.
Error If Match	Enter a string of text to check for in the returned page. If the text is contained in the page, the monitor displays content error found. HTML tags are part of a text document, so include them if they are part of the text for which you are searching. **Example:** < B> Error < /B> Message You can also perform a regular expression match by enclosing the string in forward slashes, with an **i** after the trailing slash, to indicate that there is no case-sensitive matching. **Example:** /href=Doc\d+\.html/ or /href=doc\d+\.html/i **Note:** The search is case sensitive.

GUI Element	Description
Check for Content Changes	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 go into error. If you want to check for content changes, you usually want to use **compare to saved contents**. The options for this setting are: ➤ **no content checking** (default). SiteScope does not check for content changes. ➤ **compare to last contents.** The new checksum is recorded as the default after the initial error **content changed error** occurs, so the monitor returns to OK until the checksum changes again. ➤ **compare to saved contents.** 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 **content changed error** and stays in error until the contents return to the original contents, or the snapshot is update by resetting the saved contents. ➤ **reset saved contents.** 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 **compare to saved contents** mode. **Default value:** no content checking
Baseline Interval	Enter the number of monitor runs to be averaged for use as a Rolling Baseline. Rolling baselines are calculated for an interval equal to the time to complete the number of monitor runs entered here.
HTTP Version	Select this box to force SiteScope to use HTTP version 1.0 style request headers. **Default value:** HTTP 1.1
Retries	Enter the number of times that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request for is a recoverable error.

GUI Element	Description
Accept Untrusted Certs 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 SSL Connectivity in "URL Monitor Overview" on page 559.
Accept Invalid Certs for HTTPS	Check 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.
When to Encode Post Data	Determines if the Post Data is to be encoded. Select from the following options: ➤ **Use content type.** Decide to encode the post data by the content type header. If the header equals **urlencoded** then encode, otherwise do not encode. ➤ **Force URL encoding.** Always encode the post data. ➤ **Force NO URL encoding.** Do not encode the post data.
Authorization User Name	If the URL specified requires a name and password for access, enter the name in this box.
Authorization Password	If the URL specified requires a name and password for access, enter the password in this box.
Authorization NTLM Domain	Enter the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL in this step.
NTLM V2	Select this option if the URL you are accessing requires authentication using NTLM version 2.

GUI Element	Description
Preemptive Authorization	Select when the Authorization User Name and Authorization Password should be sent if SiteScope requests the target URL. ➤ **Use Global Preference.** Select to have SiteScope use the **When to Authenticate** setting as specified in the Preemptive Authorization section of the General Preferences page. ➤ **Authenticate first request.** Select to send the user name and password on the first request SiteScope makes for the target URL. **Note:** If the URL does not require a user name and password, this option may cause the URL to fail. ➤ **Authenticate if requested.** Select to send the user name and password on the second request if the server requests a user name and password. **Note:** If the URL does not require a user name and password, this option may be used. All options use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Default Authentication Username** and **Default Authentication Password** specified in the Main section of the General Preferences page are used, if they have been specified. **Note:** Preemptive Authorization does not control if the user name and password should be sent, or which user name and password should be sent.
HTTP Proxy	(Optional) A proxy server can be used to access the URL. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the URL, enter the name here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.

GUI Element	Description
Proxy Server Password	If the proxy server requires a name and password to access the URL, enter the password here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Proxy NTLM V2	Select this option if the proxy requires authentication using NTLM version 2.
Client Side Cert	If you need to use a client side certificate to access the target URL, select the certificate file using the drop down menu. Normally, this is a .pfx (.p12) type certificate that usually requires a password. You enter the password for the certificate in the **Client Side Cert Password** field. **Note:** Client side certificate files must be copied into the SiteScope/templates.certificates directory.
Client Side Cert Password	If you are using a client side certificate and that certificate requires a password, enter the password in this field.
POST Data	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. See also the Match Content box for a way to verify that the correct form response was received. If this item is blank, a GET request is performed. **Note:** This item can also be used to pass cookies with the request. **Example:** "Set-cookie:<cookieName>=<cookieValue>"
URL Content Encoding	SiteScope retrieves the correct encoding from the server response. The default value appearing in this field should not be edited. **Example:** Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.
Error If Redirected	Select this box if you want SiteScope to notify you if a URL is redirected. **Default:** SiteScope follows redirects without reporting an error.

GUI Element	Description
Show Detailed Measurement	Select this box if you want SiteScope to record a detailed break down of the process times involved in retrieving the requested URL. These times include the following: ➤ **DNS lookup time.** The time it takes to send a name resolution request to your DNS server until you get a reply. ➤ **Connection time.** The time it takes to establish a TCP/IP/Socket connection to the Web server. ➤ **Server response time.** The time after the request is sent until the first byte (rather first buffer full) of the page comes back. ➤ **Download time.** The time it takes to download the entire page.
Match Value Labels	Use this option to enter labels for the matched values found in the content. The match value labels are used as variables to access retained values from the Content Match expression for use with the monitor threshold settings. **Note:** ➤ Separate multiple labels with a comma (,). ➤ 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.

URL List Monitor Settings

Description	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. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"URL List Monitor Overview" on page 566

The Add/Edit URL List Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
URL List Name	Enter the path name 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. **Examples:** http://www.website.com/index.html http://www.website.com/main/customer/order.html http://www.website.net/default.htm http://www.Web pages.com/tech/support/ws/intro.html

Advanced Settings (Monitor Specific)

GUI Element	Description
Server	Enter the optional Server name to specify which URLs to check in the URL list. If the URLs are stored in a map format, this item is used to check a subset of the URLs from the list. **Default:** All URLs in the list are checked.
Log	Enter the path name for the log file for this monitor. For each URL checked, an entry is added to this log file. If this item is blank, a log is not created.
Error Log	Enter the path name for the error log file for this monitor. For each error retrieving a URL, an entry is added to this log file. If this item is blank, a log is not created.
Threads	Enter the number of threads to retrieve URLs. This is the number of simultaneous checks to perform. Increasing this number shortens the time for all of the URLs to be checked but also increases the load on the server.
Pause	Enter the pause, in milliseconds, between each URL check. Decreasing this number shortens the total time required to check all of the URLs but also increases the load on the server.
Retries	Enter the number of times you want SiteScope to try to reach URLs that are returning an error.
HTTP Proxy	(Optional) A proxy server can be used to access the URLs in the list. Enter the domain name and port of an HTTP Proxy Server.
HTTP Proxy User Name	If the proxy server requires a name and password to access the URL, enter the name here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.

GUI Element	Description
HTTP Proxy Password	If the proxy server requires a name and password to access the URL, enter the password here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Authorization User Name	If the URLs in the list require a name and password for access, enter the name in this box.
Authorization Password	If the URLs in the list require a name and password for access, enter the password in this box.
Timeout	The number of seconds that the URL monitor should wait for a page to complete downloading before timing-out. Once this time period passes, the URL monitor logs an error and reports an error status. If you have checked the Retrieve Frames or Retrieve Images option, SiteScope waits for these items to be retrieved before considering the page to be fully downloaded.
Use WinInet	Select this option if you want to use WinInet as an alternative HTTP client for this monitor. **Default value:** Apache Select this option to use WinInet instead of Apache when: ➤ 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 whereas Apache does not. ➤ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.

URL Sequence Monitor Settings

Description	The URL Sequence Monitor simulates a user's actions across a series of Web pages and URLs. This is particularly useful for monitoring and testing multi-page e-commerce transactions and other interactive online applications. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"URL Sequence Monitor Overview" on page 569 "Creating a URL Sequence" on page 578

The Add/Edit URL Sequence Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Name	Enter a text name for this URL Sequence Monitor instance. This text is displayed in the System Availability Management Administration and other places in the SiteScope interface. **Default:** SiteScope creates a name based on the host, system, or URL being monitored.
Frequency	Select how often the URL Sequence Monitor should perform the Web Transaction. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. **Default value:** 10 minutes. The update interval must be a minimum of 15 seconds or longer. **Note:** Many URL sequences may take a minute or more to complete. Therefore the Frequency should be set to allow enough time for SiteScope to complete the actions of the sequence.
Steps	Use the **Add Step** button to define the URL sequence steps. For details, see "URL Sequence Steps Settings" on page 887.

Advanced Settings (Monitor Specific)

GUI Element	Description
Timeout	The number of seconds that the URL Sequence Monitor should wait for the entire sequence to complete before timing-out. Once this time period passes, the URL Sequence Monitor logs an error and reports an error status.
Timeout Is Per Step	Select this box if you want to use the value entered for the Timeout above as the Timeout for each step of the sequence rather than for the entire transaction. If the step takes more than this time to complete, the URL Sequence Monitor logs an error and reports an error status.
Retrieve Images	Select this box if you want the status and response time statistics to include the retrieval times for all of the embedded images in the page. Embedded images include those referenced by 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. **Note:** 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.
Retrieve Frames	Select this box if you want SiteScope to retrieve the frames references in a frameset and count their retrieval time in the total time to download this page. Frames include those referenced by FRAME and IFRAME tags. If **Retrieve Images** is also checked, SiteScope attempts to retrieve all images in all frames. **Note:** 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.

GUI Element	Description
Use WinInet	Select this option if you want to use WinInet as an alternative HTTP client for this monitor. **Default value:** Apache Select this option to use WinInet instead of Apache when: ➤ The Apache HTTP client does not support a specific technology required to access the server you are monitoring. For example, Kerberos authentication is not supported by the Apache library, and is supported by WinInet. WinInet also supports trusted client-side certificates while Apache does not. ➤ You tried running this monitor and the Apache server returned errors. Using WinInet may solve these errors.
HTTP Proxy	(Optional) A proxy server can be used to access the URLs in the sequence. Enter the domain name and port of an HTTP Proxy Server.
Proxy Server User Name	If the proxy server requires a name and password to access the URLs in the sequence, enter the name here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Proxy Server Password	If the proxy server requires a name and password to access the URLs in the sequence, enter the password here. **Note:** Your proxy server must support Proxy-Authenticate for these options to function.
Use Cookie Persistency	Select this option if you want to share cookies between monitor runs and between configured monitors. For details, see "Sharing Cookies Between Monitor Runs and Configured Monitors" on page 588.
Load cookies from persistency	Select this option if you want to load all relevant cookies from the persistency file and add them to the list of cookies to be sent to the server. Cookies are loaded at the beginning of the monitor run.

GUI Element	Description
Save cookies to persistency	Select this option if you want to save all cookies received from the server for the current monitor run to the persistency file. Where a cookie has the same name, and its domain and path attribute string values exactly match those of an existing cookie in the persistency file, the cookie replaces the existing cookie. Cookies are saved at the end of every monitor run and the persistency file is updated.
Cookie Persistency File	Enter the path and name of the cookie persistency file.
Proxy NTLM V2	Select this option if the proxy server requires authentication using NTLM version 2.
Resume at Step, If Error	You use this option to specify a URL sequence step to execute 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 were aborted without logging out. 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.
Execute resume step and remaining steps	If the **Resume at Step** option is selected and executed, selection of this option causes SiteScope to execute that step and continue executing the other, subsequent steps until it reaches the end of the sequence.

GUI Element	Description
Show Detailed Measurements	Select this box if you want SiteScope to record a detailed break down of the process times involved in retrieving the requested URL. These include the following: ➤ **DNS lookup time.** The time it takes to send a name resolution request to your DNS server until you get a reply. ➤ **Connection time.** The time it takes to establish a TCP/IP/Socket connection to the Web server. ➤ **Server response time.** The time after the request is sent until the first byte (rather first buffer full) of the page comes back. ➤ **Download time.** The time it takes to download the entire page.
HTTP Version	Some systems may not be designed to accept HTTP 1.1 requests headers. If this is the case, select this option to have SiteScope use HTTP 1.0. **Default value:** HTTP version 1.1
Retries	Enter the number of times that SiteScope should retry the request if a recoverable error was encountered. A timeout of the request for is a recoverable error.
Accept Untrusted Certs 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 SSL Connectivity in "URL Monitor Overview" on page 559.
Accept Invalid Certs for HTTPS	Check 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.

URL Sequence Steps Settings

The following describes the settings used for each individual sequence step in the URL Sequence step 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.

GUI Element	Description
Reference Type	You use the Reference Type options to select how SiteScope progresses from one step of a URL sequence to the next. The options include: ➤ **URL.** Go to a particular URL directly ➤ **Link.** Follow a hyperlink on the page received from the previous step ➤ **Form.** Enter data into a form received from the previous step and submit the form data to an application ➤ **Frame.** Request the content of a specific frame if the previous step returned an HTML frameset. ➤ **Refresh.** Follow an automated redirection defined by a META HTTP-EQUIV="Refresh" tag. For details, see “Creating a URL Sequence” on page 578.

GUI Element	Description
POST Data (for Form)	If the URL at this step issues a POST request for a form and the user has used the **Form** 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. 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 **POST Data** text box are not encrypted and are visible to anyone. If you want to secure the value by encrypting it, use the **Post Data Password Key** and **Post Data Password Value** fields to secure the monitor as described below.
Post Data Password Key	This is the text box in which you enter the name of the field that was supplied by the URL in the **POST Data** field. It is the **name** component of the name=value pair.
Post Data Password Value	This is the text box in which you enter the value that is required when accessing the form. This is the **value** component of the name=value pair. The value is encrypted using the TDES algorithm. For example, you want to define an encrypted password to the form that the URL monitor, gmail.com sends. The site gmail.com automatically supplies information in the POST Data text box of the URL Sequence dialog box. The Post Data Password Key may vary from site to site. The Post Data Password Key provided by gmail.com is Passwd. The Post Data Password Value is the password that you provide. For details on how to enter an encrypted or unencrypted password, see “Entering an Encrypted or Unencrypted Password” on page 585.

GUI Element	Description
URL Content Encoding	SiteScope retrieves the correct encoding from the server response. The default value appearing in this field should not be edited. **Example:** Cp1252, Cp1251, Cp1256, Shift_JIS, or EUC_JP.
Match Content	Enter a string of text to check for in the returned page or frameset. If the text is not contained in the page, the monitor displays the message content match error. HTML tags are part of a text document, so include them if they are part of the text for which you are searching. This works for XML pages as well. **Example:** < B> Hello< /B> World You can also perform a regular expression match by enclosing the string in forward slashes, with a letter i after the trailing slash indicating case-insensitive matching. **Example:** /href=Doc\d+\.html/ or /href=doc\d+\.html/i 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. **Example:** /Temperature: (\d+). This returns the temperature as it appears on the page and this could be used when setting an **Error if** or **Warning if** threshold. **Note:** The search is case sensitive.
Error If Match	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 **content error found** for this step's URL. The search is the same as for the **Match Content** field described above.

GUI Element	Description
User Name (for URL)	If the URL specified for this step requires a name and password for access, enter the user name in this box. 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.
Password (for URL)	If the URL specified for this step requires a name and password for access, enter the password in this box. 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.
Authorization NTLM Domain	Enter the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL in this step.

GUI Element	Description
Preemptive Authorization	Select when the Authorization User Name and Authorization Password should be sent if SiteScope requests the target URL. ➤ **Use Global Preference.** Select to have SiteScope use the **When to Authenticate** setting as specified in the Preemptive Authorization section of the General Preferences page. ➤ **Authenticate first request.** Select to send the user name and password on the first request SiteScope makes for the target URL. **Note:** If the URL does not require a user name and password, this option may cause the URL to fail. ➤ **Authenticate if requested.** Select to send the user name and password on the second request if the server requests a user name and password. **Note:** If the URL does not require a user name and password, this option may be used. All options use the **Authorization User Name** and **Authorization Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Default Authentication Username** and **Default Authentication Password** specified in the Main section of the General Preferences page are used, if they have been specified. **Note:** Preemptive Authorization does not control if the user name and password should be sent, or which user name and password should be sent.
Delay	(Optional) Enter how long SiteScope should wait before executing the next step of the sequence.
Step Title	(Optional) Enter the text for the title of this step within the sequence monitor. The title is only displayed in the Edit URL Sequence form.

GUI Element	Description
When to Encode Post Data	Determines if the Post Data is encoded. Select from the following options: ➤ **Use content type.** Decide to encode the post data by the content type header. If the header equals **urlencoded** then encode, otherwise do not encode. ➤ **Force URL encoding.** Always encode the post data. ➤ **Force NO URL encoding.** Do not encode the post data.
Client Side Cert	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 SiteScope/templates.certificates directory. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You enter the password for the certificate in the **Client Side Cert Password** field.
Client Side Cert Password	If you are using a client side certificate and that certificate requires a password, enter the password in this field.

Web Script Monitor Settings

Description	The Web Script Monitor gives you a flexible solution for virtual end-user monitoring of all your Web-based Applications. It can monitor dynamic content, test various authentication methods, and capture each step in a transaction between virtual user and Web site. This can help identify performance and availability issues before they impact end users. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Important Information (continued)	The Web Script Monitor is an optional SiteScope feature. Additional licensing is required to enable this monitor type in the SiteScope interface. Contact your HP sales representative for more information. **Note to HP Business Availability Center users**: The Web Script Monitor is not available when working in HP Business Availability Center and cannot be configured in System Availability Management. The monitor's data cannot be reported to HP Business Availability Center.
Useful Links	"Web Script Monitor Overview" on page 589

The Add/Edit Web Script Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Name	Enter a text name for this Web Script Monitor instance. This text is displayed in various locations in the SiteScope interface to identify the monitor.
Frequency	Select how often the Web Script Monitor should run the script. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. **Note:** The update interval must be a minimum of 15 seconds or longer.

GUI Element	Description
Web Script File Path	Select from the following options: ➤ **Full path Web script name**. 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. ➤ Web script files list. Select from the list of available scripts in the directory storing your VuGen scripts. This could be the default directory <SiteScope root directory>/templates.webscripts or a directory you name in General Preferences. For details, see "SiteScope General Preferences" on page 226. 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. ➤ 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. ➤ Each script used for a Web Script Monitor must have a unique name.
Web Script Timeout	Enter the time in seconds after which you want SiteScope to stop running the script if it has not successfully completed its run. This value must be less than the value you entered for the Frequency setting.

Part V

Integration Monitors

42

Working with SiteScope Integration Monitors

Integration Monitors enable you to capture and forward data from several Enterprise Management Systems (EMS) applications and servers into HP Business Availability Center.

Integration Monitors

Integration Monitors are run by the SiteScope data collector and are used to integrate data from third-party applications (typically EMS systems) into HP Business Availability Center.

Note: Access to Integration Monitor types requires that a special SiteScope Optional License be entered on the SiteScope server.

There are two levels of configuration for collecting the data and forwarding that data to HP Business Availability Center:

- Required: The monitors must be configured to properly map to the monitored system and collect the required samples, whether in the form of events, measurements, or tickets. The field mapping from the monitored system is done by selecting a sample type in the Field Mapping setting and editing the corresponding script template.
- Optional: The data can also be mapped to a topology to forward data to the correct CI hierarchy in HP Business Availability Center. This enables the monitor to accurately report status to the appropriate CIs within HP Business Availability Center for use by the different applications in the product. The topology settings are configured using a Jython script that is loaded depending on the type of topology you want to create.

This section includes the following topics:

- "Integration Monitor Categories" on page 900
- "Field Mapping Sample Types" on page 901
- "Topology Settings" on page 903

Integration Monitor Categories

Integration monitors can be divided into two categories.

Application-Specific Monitors

These integration monitors are designed for use with specific EMS applications. These monitors are predefined with the appropriate field mapping and topology settings.

The monitors include:

- HP OVO Event Monitor
- HP Service Center Monitor
- NetScout Event Monitor

The scripts for both the field mapping and the topology settings can be further configured to suite the needs of your specific environment.

Note: Topology Settings are not available for the NetScout Event Monitor.

Generic Integration Monitors

Technology Integration Monitors designed for use with most EMS applications that support extraction of data from a database, log file, SNMP trap, or Web service interface.

The field mapping and topology settings for these monitors must be configured by loading the applicable scripts and editing them during monitor creation.

The monitors include:

- Technology Database Integration Monitor
- Technology Log File Integration Monitor
- Technology SNMP Trap Integration Monitor
- Technology Web Service Integration Monitor

Field Mapping Sample Types

The integration monitors use field mapping scripts to correctly map the data they collect to a format recognizable by HP Business Availability Center. For the generic integration monitors, you configure and customize these mappings as required.

The mappings for the application-specific monitors are not editable while configuring the monitor and it is recommended to use the out-of-the-box integration mappings already configured for those monitors.

When configuring the generic integration monitors, select from the following types of sample scripts:

- **Measurements.** Used to collect time-based data. Data collected by Integration Monitors that use the measurements sample type is integrated into HP Business Availability Center as typical SiteScope data and can be viewed in all contexts that support viewing SiteScope data (for example, Dashboard, Service Level Management, System Availability Management, user reports, and so on). Topology settings are not available when selecting the **Measurements** field mapping.
- **Events.** Used to collect data on specific events. Data collected by Integration Monitors that use the event sample type is integrated into HP Business Availability Center using the UDX framework and can be viewed in contexts that support the display of UDX data (Event Log, Dashboard, trend reports). The data can also be accessed using the HP Business Availability Center API.
- **Tickets**. Used to collect incidents and events from ticketing systems. Data collected by integration monitors that use the ticketing sample type is integrated into HP Business Availability Center and can be viewed in Dashboard and Service Level Management.

The Database, Log File, SNMP Trap, and Web Service Technology Integration Monitors can be configured to work with these sample types. You use the field mapping script templates that come prepackaged with SiteScope as a basis for creating a customized configuration appropriate for your specific environment. When you configure an integration monitor, you select the sample type to load the appropriate script template and edit the script template in a text editor. You then copy back the edited version of the script into the monitor's field mapping setting.

For details on customizing the field mapping scripts, see "Integration Monitor Field Mapping" on page 973.

Topology Settings

To establish the full integration with Business Availability Center if you selected **Events** or **Tickets** as the field mapping for the monitor, you select a topology template for your integration monitor. You do this while creating an integration monitor in the Topology Settings area. The topology templates for **Hosts, Hosts-Applications**, and **Tickets** are specially configured with the necessary values to forward data to the appropriate CIs in Business Availability Center's CMDB.

The topology is written as a Jython script. Jython is a language based on Python and powered by Java. For details on how to work in Jython, you can refer to these Web sites:

- http://www.jython.org
- http://www.python.org

The script includes the basis of the functions necessary to retrieve the appropriate topology data from the monitored application. To build the topology, the script uses the sample that was created as a result of the monitor's field mapping. The script includes the mapping to forward the retrieved data to the relevant CIs in Business Availability Center.

SiteScope forwards the topology to create or update a CI under the following conditions:

- When the CI is created in SiteScope for the first time as a result of the monitor retrieving data, regardless of whether the CI exists in the CMDB.
- If there were any changes to any of the CI's properties.
- The initial monitor run after SiteScope is restarted.

This prevents overloading the CMDB with CI updates coming from the monitor.

Selecting a Topology

When working with application-specific monitors, you do not select a topology and the topology is preconfigured with the necessary data for the integration. If you selected **Measurements** as the monitor's field mapping, you also do not select a topology.

When working with generic integration monitors with field mapping of either events or tickets, you select from the following topology settings:

- **Custom**. You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or application CIs.

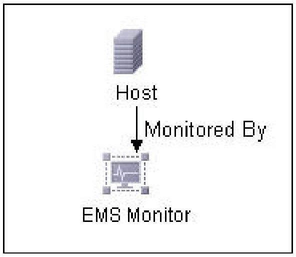
Note: It is recommended not to select **Custom** as this does not load a script and you must enter the entire script yourself. It is recommended to begin with either **Hosts** or **Hosts-Applications** and edit one of those scripts.

- **Hosts**. Creates a host CI with an EMS monitor CI as a leaf node.
- **Hosts-Applications**. Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI under the application CI. The host CI can also have an EMS monitor CI as a leaf node.
- **Tickets**. Creates a business service CI with an EMS monitor CI as a leaf node.

Note: The topology script must include the EMS monitor CI as the lowest leaf in the topology created by the integration.

Hosts Topology

The default topology created includes a Host CI with an EMS Monitor CI as its leaf node.



The Host CI has a monitored by relationship with the EMS Monitor CI. The EMS Monitor CI passes status onto the Host CI.

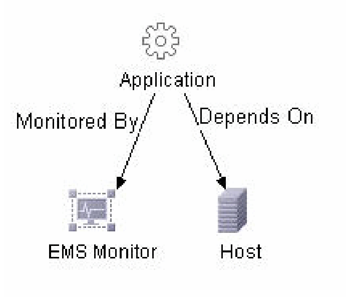
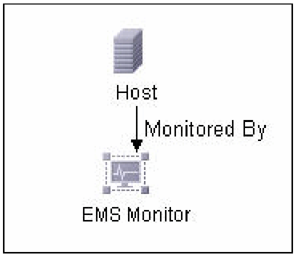
Hosts-Applications Topology

In this topology, there are two types of data that can be retrieved from the monitored system: **application** events and **system** events.

- **Application events**. This data is recognized as data affecting business services. (This event is mapped to the Application KPI for the relevant CIs.)
- **System events**. This data is all other data retrieved from the monitored application that does not affect business services. This data passes status onto the Host CI. The status may propogate to the Application CI if there is a relationship between the Host CI receiving the system event and the Application CI. (This event is mapped to the System KPI for the relevant CIs.)

If the samples forwarded belong to the category of business application events, then the status from the event is assigned to the Application CI and the Host CI does not get the status from the EMS monitor CI.

The following table illustrates the topology created for each type of event:

Topology Created for Application Event	Topology Created for System Event
 Application Monitored By Depends On EMS Monitor Host	

If the events do not belong to the category of business application events, then the event is considered a system event.

You can configure which data is considered business application data and which data is not. You configure these instructions by editing the topology script as follows:

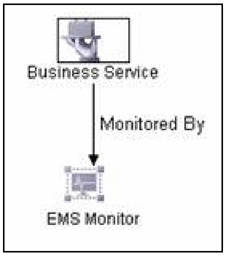
Search for the following strings in the topology script:

### EDIT THIS: Application CIs are created for all applications except "system"
if (subject != "system"):

The variable **subject** represents the subject field in the retrieved sample (as defined in the field mapping for events). The value **system** is an example of possible values representing the data from an application that is considered ‘system’ data and not forwarded to the Application CI. This ‘system’ data is forwarded to the Host CI.

Tickets

The default topology created includes a Business Service CI with an EMS Monitor CI as its leaf node. The Business Service CI has a monitored by relationship with the EMS Monitor CI.



The EMS Monitor CI passes status onto the Business Service CI.

Editing the Topology Script

To configure the topology, you must edit the Jython script that appears in the Topology Settings area when creating an integration monitor. It is highly recommended that you copy the contents of the script into your preferred text editor, edit the script in the text editor, and then copy back the contents into the Topology Settings field for the monitor.

The **Hosts**, **Hosts-Applications**, and **Tickets** topologies are already configured with the necessary information. Following are the guidelines for editing the script if you want to create your own topology.

- It is highly recommended that you familiarize yourself with the Jython language before attempting to edit this script.
- The Jython language is sensitive to spaces and tabs and you must be careful while editing the script.
- You must leave the import section as is and only add to it.
- The main body of the script is mandatory and consists of:

  ```
  def DiscoveryMain(Framework)
  ```

  This main function is responsible for creating Object State Holder Vector (OSHV) results. This holds the CI data and how to map the incoming samples to the CIs.

- Each CI should have only one EMS Monitor CI as a leaf node.
- For event scripts, the following expressions must appear as the last lines in the script:

  ```
  Framework.setUserObject("result_object",monitoredCiType)
  return OSHVResult
  ```

  The variable monitoredCiType is the CI type being monitored by the EMS Monitor CI that receives the event.

  If the script creates more than one EMS Monitor CI for one retrieved event, you must determine to which of the CIs that event belongs and passes status. You do this by assigning the correct value to the monitoredCiType. For example, if the script creates one EMS Monitor CI for an Application CI and one for a Host CI, and you want the event to pass status to the Host CI, the value of the variable monitoredCiType should be “host”.
- Use the built-in “logger” to debug the topology scripts when samples arrive. You do this by modifying the level and type of information reported to the log file. Change the log file settings in the <**SiteScope root directory**>**\conf\core\Tools\log4j\PlainJava\log4j.properties** file as follows:

  a Open the **log4j.properties** file in a text editor and locate the following lines in the file:

  ```
  # Jython prints
  log4j.category.PATTERNS_DEBUG=${loglevel}, integration.appender
  ```

  Change the argument of **log4j.category.PATTERNS_DEBUG** from **${loglevel}** to **DEBUG**, as follows:

  ```
  log4j.category.PATTERNS_DEBUG=DEBUG, integration.appender
  ```

  b Save the file. It may take a few seconds for the changes to take effect.

  The results are logged to the **bac_integration.log** file.

Jython Properties File

The <**SiteScope root directory**>/**conf/ems/jython.properties** file controls many aspects of the Jython script. Generally, you do not need to edit this file. It already includes all the properties necessary for running the Jython script.

If you working in a secure Business Availability Center installation that has a certificate, you may have to modify one of the properties in this file. In this case, you must insert the following line into the file:

```
appilog.agent.Probe.BasicAuth.Realm=MyPrivateFile
```

Where myPrivateFile is a variable for the certificate realm. If you want to find out what realm a given URL belongs to, you can open the URL with a Web browser and see the first line in the popup box.

Note: When you modify the **jython.properties**, you must restart SiteScope to enable your changes to take effect.

List of Deprecated Integration Monitors

In SiteScope version 8.5, a number of Integration Monitors were deprecated and are no longer supported.

The following Technology Integration Monitors can be used instead of the deprecated monitors:

Deprecated Monitor:	Recommended Monitor:
Avalon Event	Technology SNMP Trap
BMC Patrol Event	Technology SNMP Trap, Technology Log File
BMC Patrol	Technology Log File
CA Unicenter Event (1)	Technology SNMP Trap

Deprecated Monitor:	**Recommended Monitor:**
Compaq Insight Manager Event (2)	Technology Database
HP Systems Insight Manager Event	Technology Database
Netcool Event	Technology SNMP Trap
NetIQ (3)	Technology Database
Remedy Ticketing	Technology Database
Tivoli TEC Event	Technology Database
Tivoli DM	Technology Database
WhatsUp Event (4)	Technology Log File

The following are examples of how a Technology monitor can be configured to replace a deprecated monitor:

(1) Configure CA Unicenter agents to send SNMP traps to a SiteScope host machine where a Technology replacement monitor has been configured.

(2) For Compaq Insight Manager version 7.0, configure the replacement SiteScope monitor to read from the following tables: Notices, NoticeType, Devices, StringResource, and StringTableLarge.

(3) For NetIQ versions 5.0 and 5.1, configure the replacement SiteScope monitor to query tables Data (contains raw data) and DataHeader (contains metadata about the objects that NetIQ monitors).

(4) For WhatsUp version 8.0, configure the replacement SiteScope monitor to read from the log file EV-<date>.tab.

Note: Beginning with SiteScope 8.x, the monitor configuration file **main.config** is no longer used. All features that were supported in main.config are now supported in **event.config** and available in the **Fields Mapping** setting.

Deploy Integration Monitors

You can deploy integration monitors while working in:

- System Availability Management Administration
- EMS Integrations Admin which opens System Availability Management Administration
- A standalone SiteScope that reports to Business Availability Center

Select a SiteScope

When in System Availability Administration, select the SiteScope server from which you want to deploy the integration monitor.

For details, see "System Availability Management Administration" on page 40.

Note: This step is relevant only for users accessing SiteScope from HP Business Availability Center.

Create a Group for the Integration Monitor

It is highly recommended that you create special groups for the integration monitors. This enables you to more easily recognize the data that is reported to Business Availability Center as coming from the integrations.

For details, see "SiteScope Group Settings" on page 617.

Configure the Integration Monitor

You must configure the monitor and add the required data for the monitor's settings. You can choose from the following application-specific integrations:

- HP OVO Event Monitor
- HP Service Center Monitor
- NetScout Event Monitor

You can choose from the following generic integration monitors:

- Technology Database Integration Monitor
- Technology Log File Integration Monitor
- Technology SNMP Trap Integration Monitor
- Technology Web Service Integration Monitor

Edit Field Mappings and Topology Script

For generic integration monitors or any special customizations, you must also:

- Edit the fields mapping. For details, see "Integration Monitor Field Mapping" on page 973.
- Edit the topology settings. For details, see "Topology Settings" on page 903.

Troubleshooting Integration Monitors

The information below describes basic troubleshooting techniques and information regarding log files that may be useful when working with Integration Monitors. Additional troubleshooting information is located in the Knowledge Base on the Customer Support Web site and in the following sections:

- "Troubleshooting the Technology Database Integration Monitor" on page 946
- "Troubleshooting the Technology Log File Integration Monitor" on page 952
- "Troubleshooting the Technology SNMP Trap Integration Monitor" on page 960
- "Troubleshooting the Technology Web Service Integration Monitor" on page 968

Integration Monitor Logs

Integration Monitor activity is logged to <**SiteScope root directory**>**logs****RunMonitor.log and bac_integration.log**.

You can modify the level and type of information reported to the log file by changing the log file settings in the <**SiteScope root directory**>**conf****core****Tools****log4j****PlainJava****log4j.properties** file. You can instruct the logging mechanism to:

- report logged information in less or greater detail than is reported by default
- log all samples sent by Integration Monitors to HP Business Availability Center
- log all received events from external EMS systems

To modify log settings:

1. Open the **log4j.properties** file in a text editor.
2. To specify that samples sent by Integration Monitors to HP Business Availability Center be logged:

   a Locate the following lines in the file:

   ```
   log4j.category.EmsSamplePrinter=${loglevel}, integration.appender
   log4j.additivity.EmsSamplePrinter=false
   ```

   b Change the argument of **log4j.category.EmsSamplePrinter** from **${loglevel}** to **DEBUG**, as follows:

   ```
   log4j.category.EmsSamplePrinter=DEBUG, integration.appender
   ```

   c Save the file. It may take a few seconds for the changes to take effect.

   The results are logged to the bac_integration.log file.

3. To specify that all received events from external EMS systems be logged:

   a Locate the following lines in the file:

   ```
   log4j.category.EmsEventPrinter=${loglevel}, monitors.appender
   log4j.additivity.EmsEventPrinter=false
   ```

   b Change the argument of **log4j.category.EmsEventPrinter** from **${loglevel}** to **DEBUG**, as follows:

   ```
   log4j.category.EmsEventPrinter=DEBUG, monitors.appender
   ```

   c Save the file. It may take a few seconds for the changes to take effect.

   The results are logged to the **RunMonitor.log** file.

Other Log and Troubleshooting Issues

- Look for errors in **<SiteScope root directory>\logs\error.log** and in **<SiteScope root directory>\logs\bac_integration.log**.
- If samples are created and sent from SiteScope but cannot be seen in HP Business Availability Center Dashboard, Event Log, or SiteScope reports, search for the string ERROR or WARN in the **wde.log** and **loader.log** files in the **<HP Business Availability Center root directory>/log/mercury_wde/** directory to make sure the samples were not dropped due to missing fields or values.

- Increase the level of Dashboard logging in **<HP Business Availability Center root directory\conf\core\Tools\log4j\EJB\ble.properties** file to verify that Dashboard is receiving samples. Locate the following parameter and change the log level status to **DEBUG**:

  ```
  log4j.category.Trinity.BLE_SAMPLES=DEBUG, trinity.samples.appender
  ```

  The results are logged to the **<HP Business Availability Center root directory\log\EJBContainer\TrinitySamples.log**.

Note: Once you have determined the cause of the problem, it is recommended that you set log levels to their default settings so as not to overload the system.

43

HP OVO Event Monitor

The HP OVO Event Monitor allows you to integrate an existing Hewlett-Packard OVO Server with HP Business Availability Center by transferring HP OVO events from HP OVO Server to an HP Business Availability Center server.

Note: This monitor supports:

- HP OVO/UNIX versions 8.x (x >= 24) when installed on Solaris or on HP UX platforms.
- HP OVO/Windows versions 7.5x when installed on Windows platforms.
- English only. It does not support I18N mode.

About the HP OVO Event Monitor

The HP OVO Event Monitor depends on an HP OVO Integration Add-on module to collect events from the HP OVO Server. The Add-on, when installed on the HP OVO Server, listens to events received by the HP OVO system and sends them to the HP OVO Event Monitor. The HP OVO Event Monitor transfers the events to an HP Business Availability Center server. The HP OVO Integration Add-on and the HP OVO Event Monitor communicate using TCP/IP networking (with a customizable TCP port).

Configuration Files

The HP OVO Event monitor uses a predefined configuration file, <**SiteScope root directory**>**\conf\ems\hp\event.config**, to define the processing of incoming data and to define the output sample forwarded to HP Business Availability Center. Do not modify this configuration file.

The following configuration file allows mapping between HP OVO event fields and HP Business Availability Center KPIs and can be modified: <**SiteScope root directory**>**\conf\ems\hp\spi2kpi.config**.

Note: If you customized this file in previous versions of SiteScope, you must manually copy this file to your SiteScope version 9.0 installation. Use the same file path as in the previous version.

There are 4 sections in this file: **system**, **network**, **application**, and **security**. These sections correspond to four predefined KPIs in HP Business Availability Center for HP OVO events. You can modify this file to meet the needs of your site.

Below is a sample **spi2kpi.config** file:

```
[system]

[network]
Application1=.*SNMP*

[application]
Application1=.*MS SQL.*
Application2=.*Oracle.*
Application3=.*Informix.*
Application4=.*Sybase.*
Application5=.*Apache.*
Application6=.*iPlanet.*
Application7=.*SUN One.*
Application8=.*MSExchange.*
Application9=.*Microsoft Exchange Server.*
Application10=.*Active Directory.*
Application11=.*IIS.*
Application12=.*WebLogic.*
Application13=.*WebSphere.*
Application14=.*Biztalk.*
Application15=.*SharePoint.*
Application16=.*R3.*

[security]
Group1=.*SECURITY.*
```

Every HP OVO event is processed and matched against the regular expression pattern:

- Application<number> pattern means that an application field from the event should be matched against the regular expression pattern.
- Group<number> pattern means that the group field from the event should be matched against the regular expression pattern.

The matching process starts at the beginning of the file and proceeds line by line until the first match is found. When a match is found, the process stops and the value of the resulting KPI is assigned to the attr1 field of the event sample. If there is no match, the system KPI is assigned to the attr1 field.

The order in which you list the applications and groups in this file is important because, in the event that there may be more than one match, the parser stops after the first match. For details, see “Integration Monitor Field Mapping” on page 973.

Important: After you modify **spi2kpi.config** file, right-click the HP OVO monitor in the monitor tree, select **Edit**, and then click **OK** to close the edit monitor page. If this is not done, your changes in the configuration file are not implemented in the monitor.

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 OVO Alert Monitor Configuration Form.

For information on Integration Monitor logging and troubleshooting, see “Integration Monitor Logs” on page 913 and “Troubleshooting Integration Monitors” on page 913.

Configuring This Monitor

For details on configuring this monitor, see “HP OVO Event Monitor Settings” on page 1000.

Working with the HP OVO Integration Add-on

The purpose of the HP OVO Integration Add-on is to connect to the HP OVO message infrastructure, to receive events from the HP OVO, and to forward these events to the SiteScope machine.

Note: The HP OVO Integration Add-on module is platform specific. Modules are provided for all platforms supported by OVO/UNIX version 8.24 or OVO/Windows version 7.5.

This section includes the following topics:

- "Installing the HP OVO Integration Add-on" on page 921
- "Configuring the HP OVO Integration Add-on" on page 923
- "Tuning the HP OVO Integration Add-on" on page 924
- "Starting and Stopping the HP OVO Integration Add-on" on page 926
- "Uninstalling the HP OVO Integration Add-on files from the HP OVO Server" on page 927
- "Support in HP OVO Cluster Installation" on page 928
- "Log File Messages" on page 928

Installing the HP OVO Integration Add-on

Installation packages for the various platforms used below is in <**SiteScope root directory**>**\conf\ems\hp\addon\OVO-BAC.zip** file.

To install on HP-UX 11.11:

1. Log in as superuser to the HP OVO Server. Alternatively, use the su command to gain superuser permissions.
2. Copy **HPOvOBac-01.00.000-HPUX11.0-release.depot** installation package to **/tmp**.
3. Do the following command:

```
swinstall -s /tmp/HPOvOBac-01.00.000-HPUX11.0-release.depot \*
```

To install on HP-UX 11.23:

1. Log in as superuser to the HP OVO Server. Alternatively, use the su command to gain superuser permissions.
2. Copy **HPOvOBac-01.00.000-HPUX11.22_IPF32-release.depot** installation package to **/tmp**.
3. Do the following command:

```
swinstall -s /tmp/HPOvOBac-01.00.000-HPUX11.22_IPF32-release.depot \*
```

To install on Solaris 5.7 or later:

1. Log in as user root to the HP OVO Server. Alternatively, use the su command to gain super-user permissions.
2. Copy **HPOvOBac-01.00.000-SunOS5.7-release.sparc** installation package to **/tmp**.
3. Do the following command:

```
pkgadd -d /tmp/HPOvOBac-01.00.000-SunOS5.7-release.sparc HPOvOBac
```

To install on Windows:

1. Log in as user administrator to the HP OVO Server.
2. Copy **HPOvXpl-02.61.120-WinNT4.0-release.msi** and **HPOvOBac-01.00.000-WinNT4.0-release.msi** installation packages to **C:\tmp**. Do the following commands:
   a. msiexec /I C:\tmp\HPOvXpl-02.61.120-WinNT4.0-release.msi /qn
   b. msiexec /I C:\tmp\HPOvOBac-01.00.000-WinNT4.0-release.msi /qn

Configuring the HP OVO Integration Add-on

Once installed, the HP OVO Integration Add-on must be configured on the HP OVO Server before it can be used.

To configure the HP OVO Integration Add-on on the HP OVO Server:

1. Configure the host name or IP address of the SiteScope machine on which the HP OVO Event Monitor is installed:
   ```
   ovconfchg -ns opc.bac -set TargetHost <host name>
   ```
2. Configure the port if you are using a port other than the default (9000):
   ```
   ovconfchg -ns opc.bac -set TargetHost <host name> -set TargetPort <port>
   ```

Note: If you change this setting, make sure to update the HP OVO Event Monitor.

HP OVO Integration Add-on for UNIX provides a feature that improves performance of internal message processing. Enabling this feature improves the performance of the HP OVO Integration Add-on (and other OVO components, such as the OVO Java GUI). This feature is disabled by default.

To enable improved HP-OVO Add-on performance on UNIX feature:

On the HP OVO Server, perform the following commands:

1. `opcsv -stop`

2.
   ```
   ovconfchg -ovrg server -ns opc -set OPCMSGM_USE_GUI_THREAD
   NO_RPC
   ```
3. `opcsv -start`

Tuning the HP OVO Integration Add-on

You can tune the HP OVO Integration Add-on by running utilities from the command line on the HP OVO Server.

To check the current settings:

```
ovconfget opc.bac
```

To change a parameter:

```
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.
MinWaitTime	15	If the connecting to the SiteScope receiver failed, the HP OVO 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.

Variable Name	Default Value	Description
MaxWaitTime	120	Maximum number of seconds to wait after connection failures before retry. When doubling the wait time after connection failures exceeds MaxWaitTime, the wait time is no longer doubled and MaxWaitTime is used instead.
MaxQueueLen	1000	If the connection to the SiteScope receiver has been lost and new messages or message changes come in, these messages and message changes are buffered in a memory queue. If the number of entries in that queue reaches MaxQueueLen, the oldest entries are removed from the queue.
NodeKeepTime	900	The HP OVO Integration Add-on looks up IP addresses from host names. In addition, OVO/Windows host names also need to be looked up from the OVO database. These IP addresses (and host names on OVO/ Windows) are stored in a memory cache. Since 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 OVO Integration Add-on. There is no need to stop and restart the HP OVO Integration Add-on process.

Starting and Stopping the HP OVO Integration Add-on

The HP OVO Integration Add-on must be started after it is installed.

To start and stop the HP OVO Integration Add-on on UNIX platforms:

On UNIX platforms, the HP OVO Integration Add-on is controlled by OpenView Control Daemon (ovcd). Using the command line tool **ovc** on the HP OVO Server, perform the command:

```
ovc -stop <or start> opc2bac
```

If the HP OVO Integration Add-on disconnects from SiteScope during operation, it tries to reconnect to the SiteScope at regular intervals. In the meantime, events are stored within the HP OVO Integration Add-on.

If the HP OVO Integration Add-on terminates from SiteScope during operation, the events not yet sent to SiteScope are lost.

Note: Since the Integration Add-on is linked with HP OVO API libraries, it might be necessary to stop the Integration Add-on before installing HP OVO patches, and start it after the patch installation.

To start or stop the HP OVO Integration Add-on on Windows platforms:

On Windows platforms, the HP OVO Integration Add-on runs as a Windows service.

1 On the HP OVO Server, click **Start** > **Settings**> **Control Panel** > **Administrative Tools** > **Services**.

2 Select the service **HP OpenView Operations Message Forwarder to BAC**.

3 Click **Start** or **Stop**.

Uninstalling the HP OVO Integration Add-on files from the HP OVO Server

If you must uninstall the HP OVO Integration Add-on files from the HP OVO Server, perform the following procedure:

To remove the HP OVO Integration Add-on files from an HP OVO Server on HP-UX platform:

1. Log in as superuser.
2. Perform the command:

```
swremove HPOvOInt.HPOVOBAC
```

To remove the HP OVO Integration Add-on files from an HP OVO Server on Solaris platform:

1. Log in as superuser.
2. Perform the command:

```
pkgrm HPOvOBac
```

To remove the HP OVO Integration Add-on files from an HP OVO Server on Windows platform:

1. On the HP OVO Server, click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.
2. 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.

Support in HP OVO Cluster Installation

The HP OVO Integration Add-on is supported in an HP OVO cluster environment. You can do the following tasks:

- Install HP OVO Integration Add-on on each cluster node separately.
- Configure HP OVO Integration Add-on on each cluster node separately. All configuration settings on all cluster nodes must be identical.
- Uninstall HP OVO Integration Add-on on each cluster node separately.

Log File Messages

On UNIX platforms, the HP OVO Integration Add-on writes log messages into the log file **/var/opt/OV/logSystem.txt**.

On Windows platforms, **System.txt** is in directory <**DataDir**>**\log** where <DataDir> is the data directory chosen during OVO/Windows installation (for example, C:\Program Files\HP OpenView\Data).

Log file entries use the process name **opc2bac** for messages logged by the HP OVO Integration Add-on.

44

HP ServiceCenter Monitor

The HP ServiceCenter Monitor enables you to integrate Incident Management data from an HP ServiceCenter installation with HP Business Availability Center.

Note: This monitor supports ServiceCenter version 6.2.1.

About HP ServiceCenter Monitor

Use the HP ServiceCenter monitor in SiteScope to integrate the incident data from HP ServiceCenter' Incident Management to HP Business Availability Center.

Incident Management automates reporting and tracking an incident, or groups of incidents, associated with a business enterprise. Incident Management enables you to identify types of incidents, such as software, equipment, facilities, network, and so on, and track the resolution process of these incidents.

The HP ServiceCenter monitor forwards business service-related incidents to HP Business Availability Center to create configuration items (CIs) based on those incidents. By default, CIs are created only for those incidents that are considered business service incidents in HP ServiceCenter. If necessary for your environment, you can configure the integration scripts to map other incidents as well.

The integration maps the incidents to the business service CIs created and creates a monitored by relationship between the HP ServiceCenter monitor CI and the business service CI. The monitor integrates the incident data into samples which are forwarded to HP Business Availability Center applications, such as Dashboard and Service Level Management.

Example Integration

When an incident is opened in ServiceCenter on a service, reporting that the service is unavailable, it is forwarded to HP Business Availability Center by the SiteScope monitor. The following happens in Business Availability Center:

- The Business Service CI is created with an EMS Monitor CI if it did not already exist.
- If the Business Service CI did exist, the incident is added to the existing CI along with an EMS Monitor CI.
- You can view the service CI with this open incident in Dashboard.
- You can drill down to access HP ServiceCenter.

For more detailed information on the CIs and related KPIs, see "Integration with HP ServiceCenter" in *Using Service Level Management*.

Configuring This Monitor

For details on configuring this monitor, see "HP ServiceCenter Monitor Settings" on page 1003.

HP ServiceCenter Integration Workflow

The following are the tasks necessary to configure the integration.

Define HP ServiceCenter Tables for External Access

To enable the integration, you must provide external access to the clocks table and the probe_summary table in HP ServiceCenter. This can be done:

- Manually within HP ServiceCenter if the tables are used for other external internal integrations. For details, refer to the HP ServiceCenter documentation.
- Using the configuration file supplied with HP Business Availability Center.

To use the configuration file to enable external access to the clocks and probe_summary tables:

1. Locate the configuration file **Ticketing_Integration_extaccess_def.unl** on the HP Business Availability Center DVD and copy it to a local directory.
2. Open the HP ServiceCenter client that is attached to the server used for the the integration.
3. Select **Toolkit** > **Database Manager**.
4. In the menu on the upper right side of the Database Manager, select **Import/Load**.
5. Select the **Ticketing_Integration_extaccess_def.unl** file.
6. Click the **Load FG** button.

Edit Clocks and Incident Management Configuration Files

If any changes were made to the clocks table and/or the incident management tables in HP ServiceCenter, then the same changes must be made to the corresponding configuration files in SiteScope. The configuration files included with the integration are configured with the same parameters as the default tables in HP ServiceCenter. However, if these tables were changed in any way, they must be edited on the SiteScope side.

To edit the clocks and incident management configuration files:

1 Access the files from the following location:

   ➤ **<SiteScope root directory>/conf/ems/peregrine/incidentAttributesMapping.config**

   ➤ **<SiteScope root directory>/conf/ems/peregrine/clockAttributesMapping.config**

2 Edit the files using a text editor. Follow the mapping directions as documented in the files.

Create the JAR File

This batch file creates and compiles the files needed for the HP ServiceCenter monitor. The result of this batch is a **peregrine.jar** that is placed in the **WEB_INF/lib** directory.

To create the JAR file:

1 Stop the SiteScope service on the SiteScope machine.

2 Ensure that JDK version 1.4.1 or higher is installed.

3 Set **JAVA_HOME** system variable to the JDK directory (for example **C:\j2sdk1.4.1_03**).

4 Update the **build.properties** file with the wsdl locations. The wsdl locations are retrieved from the SC Web tier. For example, in a typical installation of Service Center, the clocks wsdl file would be: **http://<server name>:12670/Clocks?wsdl**.

5 Double-click the **<SiteScope root directory>/conf/ems/peregrine/create-peregrine-jar.bat** file to run the batch.

Note: If you are running SiteScope on a UNIX system, the file extension is **.sh** and you must run the file from the full path in a terminal window.

6 Restart the SiteScope service on the SiteScope machine.

Create a Corresponding HP ServiceCenter User

You must create a dedicated user in HP ServiceCenter that should be used solely for the purposes of this HP Business Availability Center/SiteScope integration.

The user created in HP ServiceCenter must share the same time zone as the SiteScope machine. This user must also use the same date format that SiteScope uses: **dd/mm/yy**.

Use the value for the **Username** and **Password** fields when configuring the monitor as you created in HP ServiceCenter.

Configure an HP ServiceCenter Monitor in SiteScope

You can create this monitor:

- directly in SiteScope
- using the System Availability Management Administration portal in HP Business Availability Center
- using the EMS Integrations Administration portal in HP Business Availability Center

45

NetScout Event Monitor

The NetScout Event Monitor monitors alerts received from the NetScout nGenius server and forwards them to HP Business Availability Center. This provides a way to centralize data collection, display, and alerting for the conditions for which you might otherwise be unaware until something more serious happens.

About the NetScout Event Monitor

The NetScout Event Monitor is designed to collect SNMP Trap data from NetScout nGenius servers. Each time that the monitor is run, SiteScope checks traps that have been received since the last time the monitor ran and reports the results to HP Business Availability Center.

Note: For information on Integration Monitor logging and troubleshooting, see "Integration Monitor Logs" on page 913 and "Troubleshooting Integration Monitors" on page 913.

For details on configuring this monitor, see "NetScout Event Monitor Settings" on page 1007.

System Requirements

Note: If you are upgrading SiteScope from version 7.8.1.2 or 7.9.0.0, see the note about upgrading Integration Monitor types for version 7.9.1.0 or later in "Working with SiteScope Integration Monitors" on page 899.

The following are important guidelines and requirements for using the NetScout Event Monitor to forward alerts to HP Business Availability Center.

- The NetScout nGenius server must be configured to send traps to the SiteScope server.

Note: The NetScout Event Monitor uses port 162 for receiving traps. If another application or process on the machine where SiteScope is running has bound this port, the monitor reports an **Address in use** error and the monitor type is unavailable.

- SiteScope must be registered with an HP Business Availability Center installation.The SiteScope must have a profile defined in the HP Business Availability Center installation prior to enabling the registration in the SiteScope interface. To verify registration or to re-register SiteScope with HP Business Availability Center, see the BAC Preferences page under General Preferences.
- The NetScout Event Monitor must be set to synchronize integration monitor data with HP Business Availability Center. You can use the configuration file for the NetScout Event Monitor to control the data that is sent from SiteScope to HP Business Availability Center. For details on the file structure and syntax, see "Integration Monitor Field Mapping" on page 973.

Monitor Workflow

To integrate data from a NetScout system and view the NetScout data in a way that is customized to your needs, you should follow this workflow. For details on working in HP Business Availability Center, refer to the HP Business Availability Center Documentation Library.

To integrate NetScout system data:

1. Define the NetScout Event Monitor as described in "NetScout Event Monitor Settings" on page 1007.
2. Define an appropriate dimension called Network.
3. In HP Business Availability Center access the CMDB Administration Source Manager. Create a new Generic EMS source adapter which listens to events with data_source = NetScout. Modify the source XML to fit your needs.
4. In HP Business Availability Center, access Dashboard Administration Repositories. Create a new context menu item which enables you to open the nGenius system by using the link that is sent in attr5 (one field in the sample).

46

Technology Database Integration Monitor

The Technology Database Integration Monitor allows you to collect event and time series data from database tables used by Enterprise Management Systems (EMS) by performing a query through a JDBC connection. The data retrieved is then processed and sent to HP Business Availability Center as samples (one sample for each row that was returned by an SQL query).

About the Technology Database Integration Monitor

Use the Technology Database Integration Monitor to integrate database records into HP Business Availability Center. The following are examples of data that can be integrated into HP Business Availability Center using the Technology Database Integration Monitor:

- Events from monitoring applications event tables or views.
- Open tickets from ticketing systems applications.
- Time series from monitoring applications measurement tables.

Each time the Technology Database Integration Monitor runs, it returns the monitors status, the time it took to perform the query, the number of rows in the query result set, and the first two fields in the first row of the result and writes them in the monitoring log file.

What Data Is Forwarded

The Technology Database Integration Monitor uses a user-defined query and enumerating field name, field type, and initial value. While the query provided by the user is used to define a search criterion on the database, the enumerating field is used so that events are forwarded only once. Using an initial value allows you to specify an initial threshold value for the events that should be forwarded.

For example, if **Enumerating Field Type** uses DATE and **Start from value** uses 2003-20-03 12:00:00, only events that happened after the specified date are forwarded in the first run of the monitor. In subsequent monitor runs, the highest value for the DATE field found is used to verify that only new events are forwarded.

You use the field mapping script selected for the Technology Database Integration Monitor to control the data that is sent from SiteScope to Business Availability Center. See the section on “Integration Monitor Field Mapping” on page 973 for more details on the file structure and syntax.

Before setting up the Technology Database Integration Monitor, you should be clear about the purpose and usage of the data in HP Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

Configuring This Monitor

For details on configuring the monitor, see "Technology Database Integration Monitor Settings" on page 1009.

Setup Requirements

The steps for setting up a Technology Database Integration Monitor vary according to what database software you are trying to query. The following is an overview of the requirements for using the Technology Database Integration Monitor:

- You must use one of the database drivers supplied by default, or install or copy a compatible database driver or database access API into the appropriate SiteScope directory location. The supplied drivers include:
  - **com.inet.tds.TdsDriver.** TDS driver is from i-net Software for Microsoft SQL databases. This driver is deployed with SiteScope.
  - **com.mercury.jdbc.sqlserver.SQLServerDriver.** DataDirect driver is from DataDirect Technologies. It is an alternative to the TDS driver for those Microsoft SQL databases that use Windows NT authentication. This driver is deployed with SiteScope.
  - **com.inet.ora.OraDriver.** OraDriver driver is from Oracle for Oracle databases. This driver is deployed with SiteScope.

  Other database driver packages are available as compressed (zipped) archive files or .jar files. Database drivers in this form must not be extracted. Rather, put them into the **<SiteScope root directory>\java\lib\ext** subdirectory.
- You need to know the syntax for the Database Connection URL. The Database Connection URL normally includes the class of driver you are using, some key name relating to the supplier of the driver software, followed by a combination of server, host, and port identifiers.

Database Connection URLs for this monitor are:

- **jdbc:inetdae:<hostname>:<port>**
  where <hostname> is the name of the host where the database is running and <port> is the port on which the database interfaces with the driver.
- **jdbc:mercury:sqlserver://<hosthost>:1433;DatabaseName=master; AuthenticationMethod=type2**
  where <hostname> is the name of the host where the database is running.
- **jdbc:oracle:thin:@<hostname>:<port>:<dbname>**
  where <hostname> is the name of the host where the database is running, <port> is the port on which the database interfaces with the driver, and <dbname> is the name of the Oracle database instance.

- The database you want to query must be running, have a database name defined, and have at least one named table created in the database. In some cases, the database management software needs to be configured to allow connections via 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 need to 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 appropriate queries to use.
- When adding the monitor to SiteScope, in the Main Settings area, you must select a field mapping script and load the script for the monitor. Copy the contents of the script into your preferred text editor, and edit the script to define the event handlers for this monitor instance. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 973.

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, since 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.

Step-by-Step Guide to Integrating Database Data into HP Business Availability Center

This section provides the overall flow for setting up the Technology Database Integration Monitor to work with HP Business Availability Center. If you need more information on performing any of the steps, see the sections on “Setup Requirements” on page 941, and “Technology Database Integration Monitor Settings” on page 1009.

To integrate database data into HP Business Availability Center:

1. Use a database client to connect to the relevant software database. Identify which tables contain the required events/metrics (the software schema documentation may help you with this).

2. A JDBC database driver is a prerequisite for setting up the monitor. It is recommended to use the following JDBC drivers:

   - For SQL Server:

     Database Connection URL= jdbc:inetdae:<DatabaseHostName>:<Port>?database=<Database Name>

     Database Driver=com.inet.tds.TdsDriver

- For Oracle:

  Database Connection URL= jdbc:inetora:<DatabaseHostName>:<Port>:<Database Instance Name>

  Database Driver=com.inet.ora.OraDriver

3 Use the SiteScope Database Connection tool as follows:

- Verify the driver can be loaded and that it successfully connects.
- Add a username and password to verify that a connection can be established to the database.
- Add a naive query. Refine the query until you get all the required events/metrics required for usage in HP Business Availability Center.

4 Add a Technology Database Integration Monitor in HP Business Availability Center, as described in "Technology Database Integration Monitor Settings" on page 1009. Note the following:

- 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.

5 While editing the settings for the Technology Database Integration Monitor, note the following:

- **Main Settings**. Make sure that a value is specified for all parameters in the **Main Settings** area.
- **Name.** It is recommended that the monitor name include the name of the integrated software.
- **Connection parameters.** Fill all connection parameters for connecting to the database: **Database Connection URL**; **Database User Name**; **Database Password**; **Database Driver**
- **SELECT/FROM/WHERE query clauses. SELECT** and **FROM** are mandatory. It is recommended that you build your query with the SiteScope Database Connection tool *before* defining the monitor. 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 **Advanced Settings** section for the monitor.

- **Enumerating Field parameters.** Fill in details for the enumerating field.
- **Field Mappings**. Copy the content of the field mapping script you select into a text editor, edit the script to retrieve data from the monitored application, and copy the script back into the field mapping script area. For details on editing the script, see “Integration Monitor Field Mapping” on page 973.
- **Topology Settings**. Optionally, you can configure the topology setting by creating a Jython script that creates a topology in HP Business Availability Center to match your EMS system. For details, see “Topology Settings” on page 903.

6 View the data in HP Business Availability Center:

- **Events integration.** You can view events in Dashboard (add a Generic EMS source, then add the Generic EMS NodeFactory to a view), System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- **Metrics integration.** You can view the data in any application that supports SiteScope data, including SiteScope reports.
- If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <HP Business Availability Center root directory>\bin.

To troubleshoot problems with data arriving to HP Business Availability Center, see “Troubleshooting the Technology Database Integration Monitor” on page 946.

Troubleshooting 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 **Dashboard/Event Log/SiteScope reports**, look in **<HP Business Availability Center root directory>\log\mercury_wde\wdeIgnoredSamples.log** to make sure the samples were not dropped due to missing fields or values.
- Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine: **<HP Business Availability Center root directory>\conf\core\tools\log4j\mercury_wde\wde.properties**

  Change the log level parameter to DEBUG in the following lines:

  - log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender
  - log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender

  Look at the corresponding log files:

  - **<HP Business Availability Center root directory>\logs\mercury_wde\wdeIgnoredSamples.log**
  - **<HP Business Availability Center root directory>\logs\mercury_wde\wdePublishedSamples.log**

47

Technology Log File Integration Monitor

The Technology Log File Integration Monitor watches for specific entries added to a log file of an Enterprise Management System (EMS) application by trying to match against a regular expression. From each matched entry, one sample is created and sent to HP Business Availability Center. Each time the monitor runs, it examines log entries added since the last time it ran.

About the Technology Log File Integration Monitor

The Technology Log File Integration Monitor is useful for automatically extracting data from log files and sending the data to HP Business Availability Center. For example, you can use this monitor to forward information from Hewlett Packard Network Node Manager to Business Availability Center.

Each time that it runs this monitor, SiteScope starts from the point in the file where it stopped reading the last time it ran. This insures that you are notified only of new entries and speeds the rate at which the monitor runs.

When using a regular expression to match against a specific line in the log, it is possible to use regular expression back references to select the data to be forwarded to Business Availability Center. For details on using back references, see “Retaining Content Match Values” on page 1293.

What Data Is Collected

The Technology Log File Integration monitor sends to Business Availability Center data that is extracted from any row that matched against the **Content Match** regular expression.

Before setting up the Technology Log File Integration Monitor, you should be clear about the purpose and usage of the data in HP Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

The specific data that is forwarded to HP Business Availability Center is controlled by the field mapping script. You use this script to specify the preferred value fields that you want forwarded. For more details on selecting the script and the file structure and syntax, see “Integration Monitor Field Mapping” on page 973.

Configuring This Monitor

For details on configuring the monitor, see “Technology Log File Integration Monitor Settings” on page 1017.

Setup Requirements

The following are requirements for using the Technology Log File Integration Monitor to forward data to Business Availability Center:

- You must have the format and syntax of the log file that you want to monitor. You must construct a **Content Match** regular expression to match on the entries in the log file that contain the data you want to monitor and forward to Business Availability Center. For examples of regular expressions, see “Examples for Log File Monitoring” on page 1299.
- When adding the monitor to SiteScope, in the Main Settings area, you must select a field mapping script and load the script for the monitor. Copy the contents of the script into your preferred text editor, and edit the script to define the event handlers for this monitor instance. For details on the file structure and syntax, see “Integration Monitor Field Mapping” on page 973.

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)
```

Step-by-Step Guide to Integrating Log File Data into HP Business Availability Center

This section provides the overall flow for setting up the Technology Log File Integration Monitor to work with HP Business Availability Center. If you need more information on performing any of the steps, see the sections on "Setup Requirements" on page 949, or "Technology Log File Integration Monitor Settings" on page 1017.

To integrate log file data into HP Business Availability Center:

1. 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 use.

   ➤ make sure that values extracted correctly from the line.

2. Add a Technology Log File Integration Monitor in HP Business Availability Center. Note the following:

   ➤ 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.

3. While editing the settings for the Technology Log File Integration Monitor, note the following:

   ➤ **Main Settings**. Make sure that a value is specified for all parameters in the **Main Settings** area.

   ➤ **Name.** It is recommended that the monitor name include the name of the integrated software.

- **Log File Pathname** 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 Pathname** box (SiteScope should run under a privileged user for the machine that holds the file), and leave the **Server** box empty.
- **Frequency.** Specify how often the monitor should query the log file.
- **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.
- **Field Mappings**. Copy the content of the field mapping script you select into a text editor, edit the script to retrieve data from the monitored application, and copy the script back into the field mapping script area. For details on editing the script, see “Integration Monitor Field Mapping” on page 973.
- **Topology Settings**. Optionally, you can configure the topology setting by creating a Jython script that creates a topology in HP Business Availability Center to match your EMS system. For details, see “Topology Settings” on page 903.

4 It is recommended that you perform optimization of the regular expression after completing setup of the Technology Log File Integration Monitor (for example, to check for problems with use of quantifiers such as **.***). Optimization is done with the SiteScope Regular Expression tool. Update the monitor with any corrections.

5 View the data in HP Business Availability Center:

- **Events integration.** You can view events in Dashboard (add a Generic EMS source, then add the Generic EMS NodeFactory to a view), System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- **Metrics integration.** You can view the data in any application that supports SiteScope data, including SiteScope reports.
- If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <HP Business Availability Center root directory>\bin.

To troubleshoot problems with data arriving to HP Business Availability Center, see "Troubleshooting the Technology Log File Integration Monitor" on page 952.

Troubleshooting 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 **Dashboard/Event Log/SiteScope reports**, look in <**HP Business Availability Center root directory**>**log****mercury_wde****wdeIgnoredSamples.log** to make sure the samples were not dropped due to missing fields or values.

- Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine: **<HP Business Availability Center root directory>\conf\core\tools\log4j\mercury_wde\wde.properties**

  Change the log level parameter to DEBUG in the following lines:

  - log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender
  - log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender

  Look at the corresponding log files:

  - **<HP Business Availability Center root directory>\logs\mercury_wde\wdeIgnoredSamples.log**
  - **<HP Business Availability Center root directory>\logs\mercury_wde\wdePublishedSamples.log**

48

Technology SNMP Trap Integration Monitor

The Technology SNMP Trap Integration Monitor watches for SNMP traps received by SiteScope from third-party Enterprise Management Systems (EMS). For each SNMP trap that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the SNMP trap values.

The third-party EMS systems need to be configured to send traps to the SiteScope server.

About the Technology SNMP Trap Integration Monitor

The Technology SNMP Trap Integration Monitor is useful for integrating traps that your external devices generate into the HP Business Availability Center framework. For example, you can use this monitor to forward information from Hewlett Packard Network Node Manager to Business Availability Center. See "Integration with HP Network Node Manager" on page 969 for more information.

What Data Is Collected

The Technology SNMP Trap Integration Monitor collects data that is extracted from any SNMP trap received by SiteScope and sends notifications to HP Business Availability Center containing preferred values from the original SNMP trap.

Before setting up the Technology SNMP Trap Integration Monitor, you should be clear about the purpose and usage of the data in HP Business Availability Center (for presentation in Dashboard, Service Level Management, and/or reports).

The specific data that is forwarded to HP Business Availability Center is controlled by the field mapping script. You use this script to specify the preferred value fields that you want forwarded. For more details on selecting the script and the file structure and syntax, see "Integration Monitor Field Mapping" on page 973.

Configuring This Monitor

For details on configuring the monitor, see "Technology SNMP Trap Integration Monitor Settings" on page 1026.

Setup Requirements

The following are requirements for using the Technology SNMP Trap Integration Monitor to forward data to Business Availability Center:

- When adding the monitor to SiteScope, in the Main Settings area, you must select a field mapping script and load the script for the monitor. Copy the contents of the script into your preferred text editor and edit the script to define the event handlers for this monitor instance. For details on the file structure and syntax, see "Integration Monitor Field Mapping" on page 973.

Note: All the received traps are saved to **snmptrap.log** in **<SiteScope root directory>\logs**. When referring to data arriving from the Technology SNMP Trap Integration Monitor in the config file, 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.

- 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 information on SNMP configuration.

Note: The Technology SNMP Trap Integration 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. You need to terminate the process or service that is using the port, and restart SiteScope afterwards.

Step-by-Step Guide to Integrating SNMP Trap Data into HP Business Availability Center

This section provides the overall flow for setting up the Technology SNMP Trap Integration Monitor to work with HP Business Availability Center. If you need more information on performing any of the steps, see the sections on "Setup Requirements" on page 957, and "Technology SNMP Trap Integration Monitor Settings" on page 1026.

To integrate SNMP trap data into HP Business Availability Center:

1. Configure the relevant software to send SNMP traps to the SiteScope machine.
2. Open the SiteScope SNMP Trap tool and 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: Stop SiteScope, and verify that the SNMP trap port (162) is available—**netstat –na | find "162"** shows no output. (To see which process uses this port, you can download **tcpview** from **www.sysinternals.com**.)

   If the port is busy, locate the program that uses it (often the Microsoft SNMP Trap Service) and terminate it. Restart SiteScope.
3. Add a Technology SNMP Trap Integration Monitor in HP Business Availability Center, as described in "Technology SNMP Trap Integration Monitor Settings" on page 1026. Note the following:

   - 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.
4. While editing the settings for the Technology SNMP Trap Integration Monitor, note the following:

   - **Main Settings**. Make sure that a value is specified for all parameters in the **Main Settings** area.
   - **Name.** It is recommended that the monitor name include the name of the integrated software.

- **Field Mappings**. Copy the content of the field mapping script you select into a text editor, edit the script to retrieve data from the monitored application, and copy the script back into the field mapping script area. For details on editing the script, see "Integration Monitor Field Mapping" on page 973.
- **Topology Settings**. Optionally, you can configure the topology setting by creating a Jython script that creates a topology in HP Business Availability Center to match your EMS system. For details, see "Topology Settings" on page 903.

5 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.snmplink.org.)

6 View the data in HP Business Availability Center:

- **Events integration.** You can view events in Dashboard (add a Generic EMS source, then add the Generic EMS NodeFactory to a view), System Availability Management Event Log reports, or Analytics. You can also use events when building SLAs.
- **Metrics integration.** You can view the data in any application that supports SiteScope data, including SiteScope reports.
- If you want to watch the incoming samples (to view the original data before it is passed to the applications), use the sprinter utility available under <**HP Business Availability Center root directory**>**\bin**.

To troubleshoot problems with data arriving to HP Business Availability Center, see "Troubleshooting the Technology SNMP Trap Integration Monitor" on page 960.

Troubleshooting the Technology SNMP Trap Integration Monitor

The following sections provide information on troubleshooting for the Technology SNMP Trap Integration Monitor, and verifying the communication paths:

- “Basic Troubleshooting Guidelines” on page 960
- “Verify SNMP Trap Reception to SiteScope” on page 961
- “Common Problems and Solutions” on page 962

Basic Troubleshooting Guidelines

- Check for errors in <**SiteScope root directory**>**\logs\RunMonitor.log** and in <**SiteScope root directory**>**\logs\error.log**.
- Change the log level to DEBUG in <**SiteScope root directory**>**\conf\core\Tools\log4j\PlainJava\log4j.properties**, to watch outgoing samples.

  Change the line:
  log4j.category.EmsEventPrinter=${emsloglevel}, ems.appender
  to:
  log4j.category.EmsEventPrinter= DEBUG, ems.appender.

  The log file to look at is: <**SiteScope root directory**>**\logs\RunMonitor.log**
- Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine: <**HP Business Availability Center root directory**>**\conf\core\tools\log4j\mercury_wde\wde.properties**

  Change the log level parameter to DEBUG in the following lines:

  - log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender
  - log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender

Look at the corresponding log files:

- ➤ **<HP Business Availability Center root directory>\logs\mercury_wde\wdeIgnoredSamples.log**
- ➤ **<HP Business Availability Center root directory>\logs\mercury_wde\wdePublishedSamples.log**

Verify SNMP Trap Reception to SiteScope

You can verify that SiteScope is receiving SNMP traps from other management systems using the SiteScope SNMP Trap Monitor. Use the following steps to verify that SiteScope is receiving traps.

To verify that SiteScope is receiving SNMP traps:

1. Add a SNMP Trap Monitor to SiteScope. In case you already have SNMP Trap Monitor defined, you can skip this step.
2. 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 generate traps. On some systems there is a test mode that you can use to generate 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.
3. 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 SNMP traps are not forwarded to HP Business Availability Center applications.	The SNMP Agent does not emit SNMP traps.	Verify that the SNMP Agent is configured to emit SNMP traps. Use the **SiteScope\logs\snmptrap.log** file to verify that traps are received by SiteScope. For details, see "Verify SNMP Trap Reception to SiteScope" on page 961.
	The EMS configuration file contains errors.	Click the **Test Script** button in the Advanced Settings to verify the EMS configuration file.
	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 NT or Windows 2000 OS.
	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 Dashboard/Event Log/SiteScope reports.	Samples were dropped due to missing fields or values.	Check in **<HP Business Availability Center root directory>\log\mercury_wde\wdeIgnoredSamples.log**.

49

Technology Web Service Integration Monitor

The Technology Web Service Integration Monitor enables a Web service entry point to SiteScope. The monitor can be used to report data from third-party Enterprise Management Systems (EMS) to SiteScope through Web service. Both event and metrics entry points into HP Business Availability Center are published for external systems to use. For each event and/or metric that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the event and/or metrics values.

About the Technology Web Service Integration Monitor

Use the Technology Web Service Integration Monitor for integrating event data or metrics data from your existing EMS system to HP Business Availability Center. SiteScope supplies a WSDL file which the user can use to create a client code. The client code reports the event and/or metrics data to SiteScope. The client has several ways to report data to HP Business Availability Center:

- report one event
- report an array of events
- report one metric
- report an array of metrics

What Data Is Collected

The Technology Web Service Integration Monitor collects data that is extracted from any message received by SiteScope report data Web service and sends notifications to HP Business Availability Center containing preferred values from the original message.

Before setting up the Technology Web Service Integration Monitor, you should understand and map out the purpose and usage of the data that is forwarded to HP Business Availability Center. You should determine if the data is for presentation in the Dashboard, Service Level Management, and/or reports.

The specific data that is forwarded to HP Business Availability Center is controlled by the field mapping script. You use this script to specify the preferred value fields that you want forwarded. For more details on selecting the script and the file structure and syntax, see “Integration Monitor Field Mapping” on page 973.

Limitations

If you are working with HP Business Availability Center version 5.1 and lower, you cannot define new Technology Web Service Integration monitors or edit existing ones from within HP Business Availability Center. If you need to define a new Technology Web Service Integration monitor or edit an existing monitor, detach SiteScope from HP Business Availability Center, define the monitor in SiteScope's new user interface, and then attach the SiteScope to HP Business Availability Center again.

Configuring This Monitor

For details on configuring the monitor, see "Technology Web Service Integration Monitor Settings" on page 1031.

Setup Requirements

- When adding the monitor to SiteScope, in the Main Settings area, you must select a field mapping script and load the script for the monitor. Copy the contents of the script into your preferred text editor and edit the script to define the event handlers for the monitor instance. For details on the file structure and syntax, see "Integration Monitor Field Mapping" on page 973
- To enable the connection to SiteScope reportMonitorData Web service, you must create a client code (in any language) that makes the connection and handles the reporting of the data to SiteScope through the Web service.

To enable the connection to SiteScope reportMonitorData Web service:

1 Open Explorer and go to SiteScope (http://<SiteScope host>:8080/SiteScope/services). Take the WSDL file of the service **reportMonitorData**. The WSDL is an interface file which represents the API of the reportMonitorData Web service in SiteScope. The reportMonitorData service is the service that listens to incoming messages and forwards them to HP Business Availability Center. This file is used to create the client stubs that connect to the service and report the data.

2 Generate the stubs using the WSDL file. The generation of the stubs can be to any language. The way to generate the files depends on the language that you want to use.

   For example, if you want to use Java as the client code, you must use the WSDL2JAVA task in AXIS package that can be downloaded from their Web site. Run **Java org.apache.axis.wsdl.WSDL2Java <name of saved WSDL file**>. After running this, you get two packages. One package is **com**, which holds the needed objects for sending the data, and the second is **localhost**, which holds the stubs that makes the connection to SiteScope Web service.

3 Write the actual client code which uses the generated classes to send the data to SiteScope. In the code, call the **setreportMonitorDataEndpointAddress(<SiteScope targetHost>)**, which is found in **MonitorDataAcceptorServiceLocator** (one of the generated stubs) to set the SiteScope address to where you want the data reported.

4 Run your code and check if you get data in the SiteScope Technology Web Service Integration monitor.

Check Connectivity to the Technology Web Service Integration Monitor

After creating a Technology Web Service Integration monitor in SiteScope, you can check connectivity to the Web service by using the **test_client** which is located in the <**SiteScope root directory**>**conf****ems****webservice****test_client** directory. This tool sends constant messages to SiteScope reportMonitorData Web service. The messages can be either metrics messages or event messages.

To use the client tool to check connectivity:

1 In the <**SiteScope root directory**>**conf****ems****webservice****test_client** directory, run the **test_event_client.bat** for events or **test_metrics_client.bat** for metrics, using the following parameters:

- **Target Host.** The address of the SiteScope host which receives the messages.
- **Number of messages to send.** Number of messages to send to SiteScope.
- **System Id.** System Id of the monitor that receives the messages.
- **Severity/Quality.** Severity of the event when forwarding events (default is to send 1 to 5). Quality of the metric when forwarding metrics data (default is 0-3).

2 If you are forwarding other values to HP Business Availability Center, you must edit the configuration file accordingly.

The tool can also be executed with no parameters. In this case, the tool tries to send one message to the local host. The message has the system id: **Test Event System Id**. The severity is 5 (for events) or the quality is 3 (for metrics).

If you use this option, you must activate it on the SiteScope machine and have a Technology SNMP Trap Integration monitor with the system id: **Test Event System Id**.

3 After running the tool, go to the appropriate SiteScope monitor and see if the number of messages received equals the number that you sent. In addition, you can go to one of the applications (Dashboard, System Availability Management) and see if the data that you sent is displayed.

Troubleshooting the Technology Web Service 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 **Dashboard/Event Log/SiteScope reports**, look in <**HP Business Availability Center root directory**>**\log\mercury_wde\wdeIgnoredSamples.log** to make sure the samples were not dropped due to missing fields or values.
- Change the logging level for Dashboard to verify that Dashboard received the samples. Open the following file on the Gateway Server machine: <**HP Business Availability Center root directory**>**\conf\core\tools\log4j\mercury_wde\wde.properties**

  Change the log level parameter to DEBUG in the following lines:

  - log4j.category.com.mercury.am.platform.wde.decode.IgnoredSamplesLogger=${loglevel}, IgnoredSamples.appender
  - log4j.category.com.mercury.am.platform.wde.publish_SamplePublisherSamples=${loglevel}, PublishedSamples.appender

  Look at the corresponding log files:

  - <**HP Business Availability Center root directory**>**\logs\mercury_wde\wdeIgnoredSamples.log**
  - <**HP Business Availability Center root directory**>**\logs\mercury_wde\wdePublishedSamples.log**

50

Integration with HP Network Node Manager

HP Business Availability Center can accept events from Hewlett-Packard Network Node Manager (NNM).

About Network Node Manager Integration

You can forward from Network Node Manager (NNM) event data by configuring NNM to run a script for each event that you want forwarded to HP Business Availability Center. The script that you write and associate with NNM can do one of the following actions:

- write the NNM data to a log file
- send an SNMP trap with the NNM data to a SiteScope server

If your script writes the data to a log you then use a Technology Log File Integration Monitor to read the data and forward it to HP Business Availability Center. If you use a script to send an SNMP trap to a SiteScope server, you use an Technology SNMP Trap Integration Monitor configured to receive it and forward to HP Business Availability Center.

Writing Scripts to Export Network Node Manager Data

The script you use should accept data from Network Node Manager as a command line argument, and process the data so that it can be forwarded to HP Business Availability Center. The following sections describe example scripts that can be used to export NNM data.

Sample Script for Writing to a Log File

The following Perl script receives data from the command line and writes it to a log file as a comma separated vector of values that can be parsed by the Log File Integration Monitor:

```
#!/usr/bin/perl
open LOG, ">>log1.log" or die;
print LOG (join ',', @ARGV) . "\n";
close LOG;
```

Sample Script for Sending SNMP Trap Data

The following Perl script receives data from the command line and sends it as a message in an SNMP trap (using SNMP data generated by Network Node Manager) that can be caught by a Technology SNMP Trap Integration Monitor. It accepts the host name to which the trap is sent as the first parameter and a string description of the alert as the second parameter.

```
#!/usr/bin/perl
$host = $ARGV[0];
$message = $ARGV[1];
system("snmptrap $host \"\" \"\" 6 0 5 system.sysDescr.0 “ .
“octetstringascii $message");
```

Configuring Events in Network Node Manager

Use the following steps to configure Network Node Manager to execute a script for the requested events in Network Node Manager. The figure below shows examples of the applicable Network Node Manager pages and dialogs you use.

To configure Network Node Manager to execute scripts:

1. From the **Options** menu choose **Event Configuration.**
2. Select the requested enterprise and event from the **Event Configuration** dialog.
3. Select the Actions tab from the Edit > Events > Modify Events dialog.
4. Type the command line for the script in the **Command for Automatic Action** text box. You may use NNM variables to pass data to the command line.
5. Click **OK** to close the **Modify Events** dialog.
6. From the **File** menu in the **Event Configuration** dialog select **Save**.

51

Integration Monitor Field Mapping

You enable capturing event and metrics data from Enterprise Management Systems, automated support systems, and other management applications by configuring integration monitors and their field mapping scripts.

Integration Monitor Field Mapping

Integration monitors depend on field mappings you customize within the user interface in the settings for the monitor. The mapping defines the processing of incoming data and defines the output sample forwarded to Business Availability Center.

Integration Monitors designed for use with specific EMS applications (these currently include HP OVO, HP Service Center, and NetScout) can be configured without editing their field mapping script. The mappings are predefined by HP and require modification only if specific customizations are required. For details on editing these field mapping scripts, see the description for the field mapping element in the user interface pages for the monitor you are deploying.

For Technology Integration Monitors (Technology SNMP Trap, Technology Log File, and Technology Database monitors), you must select the sample type and the appropriate script template is loaded directly into the field mapping text box. You must edit the field mapping script to suite your organization's needs. The Technology Web Service Integration Monitor field mapping may also need to be customized. You can select from the following sample types:

- **Events**. Select to forward event data to Business Availability Center.

  When you select **Events** and you want to integrate to Business Availability Center using topology settings, it is recommended that you select from the following topology script templates: **Hosts** or **Hosts-Applications**.

- **Measurements**. Select to forward measurement data to Business Availability Center.

  When you select **Measurements,** you can not use topology settings to integrate with Business Availability Center.

- **Tickets**. Select to forward ticket data to Business Availability Center.

  When you select **Tickets** and you want to integrate to Business Availability Center using topology settings, it is recommended that you select the following topology script template: **Tickets**.

  For details, on selecting a topology setting, see "Topology Settings" on page 903.

Note: Use only the mandatory and optional fields defined in the script templates when working with the field mapping. For more information, see the tables for each sample type.

Understanding Field Mapping Structure

The field mapping contains instructions on how to process the data as it arrives to the integration monitors. The instructions that constitute the field mappings are grouped into event handlers—independent sections that contain instructions relevant to specific data. Each event handler contains a **matching condition** by which SiteScope can determine whether to use a particular event handler for an arriving event.

When an event or measurement data arrives at the integration monitor, it iterates over the different event handlers in the field mapping, in the order they appear, testing the **matching condition** of each handler. If a matching handler is found, the monitor uses the instructions within that handler to process the event and perform the action defined for this handler (for example, forward it to Business Availability Center or discard). No further sections are checked after the first match. If no matches are found, the event is discarded.

In addition to the event handlers, the field mapping can contain special entries that affect the integration monitor engine as a whole. These values are grouped into the [$DEFAULT_PARAMETERS$] section. This section defines default values for tags that are common for all handlers. Any tag can be set in this section of the field mapping. It is used to create a reported value unless overridden in the matched event handler. For each incoming event, this event handler is always executed prior to the matched event handler.

For details on event handler structure, see "Event Handler Structure" on page 989.

Configuring Field Mapping for Event Samples

The events sample type is used for extracting events collected by external systems and importing them to Business Availability Center. When configuring an integration monitor's field mapping, select the **Events** sample type to load the events script. You can then copy the contents of the **Field Mapping** text box and paste it into a text editor to make your configuration changes. When you are done, copy the contents back into the Field Mapping text box.

This section includes the following topics:

- "Mandatory Values for the Event Script" on page 977
- "Optional Values for the Event Script" on page 978
- "Conditional Expression Example 1" on page 980
- "Conditional Expression Example 2" on page 980
- "Event Script Example" on page 981

Mandatory Values for the Event Script

The tables below list mandatory and optional values for the event script.

Field Name	Type	Description	Example
time_stamp	DOUBLE	Time stamp in seconds since Jan 1 1970	time_stamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS"). time_stamp:DOUBLE=time()
severity	INT	Can be one of the following preconfigured severities (based on applicable integer): 0:SEVERITY_UNKNOWN 1:SEVERITY_INFORMATIONAL 2:SEVERITY_WARNING 3:SEVERITY_MINOR 4:SEVERITY_MAJOR 5:SEVERITY_CRITICAL	severity:INT=SEVERITY_MINOR

target_name	STRING	Name of device or host that generated the event	target_name=$hostName
			target_name=resolveHostName (String hostname)

status	STRING	Status of event in external EMS terminology	status=”OPEN”
			status=”ASSIGNED”
			status=”CLOSED”

subject	STRING	Subject of event (e.g. CPU, SAP application, Hard Disk), middle/high level hierarchy describing the event source.	subject=”DISK”

Field Name	Type	Description	Example
instance	STRING	Instance of subject that generated the event (e.g D:\). Lowest level of hierarchy describing the event source	instance=”E:\\”
description	STRING	Textual description of event	description="free space on drive e is below 10%"
data_source	STRING	System that generated the event	data_source=”HP OVO”

Optional Values for the Event Script

The tables below list optional values for the event script.

Field Name	Type	Description	Example
target_ip	STRING	IP of host or device that generated the event	target_ip=$IPString
object	STRING	Optional level in the hierarchy describing the event source	object="OS"
event_id	STRING	Unique identifier of this event	event_id=$id
logical_group	STRING	Logical grouping of this event	logical_group=”error messages”
monitor_ group	STRING	Monitor group that reported this event	monitor_group="log monitors on \\hostname"
orig_severity _name	STRING	Severity in external EMS terminology	orig_severity_name ="Cleared"
acknowledge d_by	STRING	Name of user that acknowledged this event	acknowledged_by =$username
owner	STRING	Name of user who owns this event	owner="admin"

Field Name	Type	Description	Example
value	DOUBL E	Use to transfer numerical values from the event	value=$thresholdViolated
attr1	STRING	Extra data slot	attr1=$history
attr2	STRING	Extra data slot	attr2=$moreHistory
attr3	STRING	Extra data slot	attr3="Design"
attr4	STRING	Extra data slot	attr4=$MonitorOutput
attr5	STRING	Extra data slot for long strings	attr5=$Longhistory

Host DNS Resolution for Event Sample

Both the FQDN (fully qualified domain name) and valid IP address are necessary for the fields that are used to create host CIs in HP Business Availability Center integration.

If you do not know the FQDN and/or IP address, then you can use the following functions in the field mapping to resolve the names and access them from the source of the integration:

target_name=resolveHostName($SomeHost)

target_ip=resolveHostIP($SomeHost)

Note: The variable **$SomeHost** must be replaced by a variable from the integration source.

These functions are not necessary if:

- The FQDN and/or IP address is available from the source that the integration is accessing. In this case, you should input the value for **target_name=** as a FQDN and the value for the **target_ip=** without the function.
- It is not possible for the SiteScope server to resolve the FQDN and/or IP address for the servers from the source that the integration is accessing. In this case, the functions may not provide the valid values.

Conditional Expression Example 1

```
severity:INT=$var6.equals(“red”) ? SEVERITY_CRITICAL
: SEVERITY_INFORMATIONAL
```

In this example, the value of sixth variable binding is compared to string red. If the variable binding is indeed equal to string red, then the value of the severity tag is set to SEVERITY_CRITICAL, otherwise it is set to SEVERITY_INFORMATIONAL.

Conditional Expression Example 2

```
severity:INT=$var6.equals(“red”) ? SEVERITY_CRITICAL :
$var6.equals(“green”) ? SEVERITY_INFORMATIONAL : $var6.equals(“yellow”)
? SEVERITY_MINOR : SEVERITY_WARNING
```

This example chains the conditional operator into a decision chain. If the sixth variable binding holds string red, then severity tag has the value SEVERITY_CRITICAL. If the sixth variable binding holds string green, then severity tag has the value SEVERITY_INFORMATIONAL. If the variable binding holds string yellow, the tag has the value SEVERITY_MINOR. If none of the above conditions are true, then the tag has the value SEVERITY_WARNING.

Event Script Example

In the example below, two types of events are sent: the first are events of status "OPEN" and the second are events cleared by a user. The data is retrieved from incoming event fields using the $ notation. All other events are discarded by the last handler.

```
[$DEFAULT_PARAMETERS$]
##################################################
# NOTE: the following parameters are mandatory #
##################################################
time_stamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS")
severity:INT= SEVERITY_UNKNOWN
target_name=$Device
status=$Status
subject="EMS X Events"
instance=$target
description=$description
data_source="EMS X"

#send an open event with the value in value fields and with the event id
[OPEN events]
$MATCH="OPEN".equals($Status)
$ACTION=TOPAZ_BUS_POST(event)
value:DOUBLE=parseDouble($threshold)
event_id=$uid

#send clear events with the event id and acknowledging username
[clear events]
$MATCH="CLEAR".equals($Status)
$ACTION=TOPAZ_BUS_POST(event)
event_id=$uid
acknowledged_by=$ClearedBy

[event sink]
$MATCH=true
$ACTION=DISCARD
```

Configuring Field Mapping for Measurement Samples

The measurements sample type is used for extracting metrics collected by external systems and importing them to Business Availability Center. When configuring an integration monitor's field mapping, select the **Measurements** sample type to load the measurements script. You can then copy the contents of the **Field Mapping** text box and paste it into a text editor to make your configuration changes. When you are done, copy the contents back into the Field Mapping text box.

Note: If you select the measurement field mapping, you should not use the topology settings for the integration. The topology settings are not supported for the measurement script template type.

This section includes the following topics:

- "Mandatory Values for the Measurements Script" on page 983
- "Measurements Script Example" on page 983

Mandatory Values for the Measurements Script

The table below lists mandatory values for the measurements script.

Field Name	Type	Description	Example
TimeStamp	DOUBLE	Time stamp in the seconds since Jan 1st 1970 format	TimeStamp:DOUBLE=time ()
Quality	INT	Quality in SiteScope terms. Possible values are: `QUALITY_ERROR`, `QUALITY_WARNING`, `QUALITY_GOOD`	Quality:INT= QUALITY_ERROR
MonitorName	STRING	Logical monitor name	MonitorName=”NT cpu Monitor”
MonitorState	STRING	The monitor status, for example, N\A, Good, Error, and so on.	MonitorState=”Received ” + $count + “ events”
MonitorType	STRING	The monitor type	MonitorType=”System Monitor”
TargetName	STRING	The target of this monitor (e.g. host name)	TargetName=$Device
Measurement Name(N)	STRING	Name the Nth measurement	MeasurementName(1)=”CPU Temperature”
Value(N)	DOUBLE	Value of Nth measurement	Value(1):DOUBLE=$CPU Temperature

Measurements Script Example

In the example below, two measurements are sent: the first one (MeasurementName (1)) takes its name from the $legend field and takes the value from the $value field. A second measurement (Measurement Name (2)) uses the constant name CPU Temperature which receives its value from the $CPUTemp field.

```
###########################################
#            EMS Integration metricsconfig file  #
# use this file to send metrics to HP Business Availability Center #
###########################################
[$DEFAULT_PARAMETERS$]
# time stamp in the seconds since Jan 1st 1970 format.
TimeStamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS")

# quailty in SiteScope terms QUALITY_ERROR, QUALITY_WARNING,
QUALITY_GOOD
Quality:INT=QUALITY_ERROR

# Logical monitor name
MonitorName=$kpName

#target, e.g. host name
TargetName=$parentMachineName

#the status string of the monitor (e.g.: “Log file read, 3 matches found”)
MonitorState=”The monitor status is: “+ $status

#the monitor type (e.g. “Log Monitor”, “CPU Monitor”)
MonitorType=”NetIQ measurements”

#measurement name
MeasurementName(1)=$legend
#value as double
Value(1):DOUBLE=parseDouble($value)

#measurement name
MeasurementName(2)=”CPU Temperature”
#value as double
Value(2):DOUBLE=parseDouble($CPUTemp)
######################################################
# To send more than one measurement per DB row #
# add pairs #
# MeasurementName (* ) = #
# Value (*) :DOUBLE= #
# where * = 1,2,.,n #
# ####################################################
[allR]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(ss_t)
```

When specifying more than one measurement in the script, a separate sample is sent with each of the measurements.

Note: When specifying multiple measurements per file, the measurement numbering must be consecutive.

In the case of failure, errors appear in the **RunMonitor.log** but the error does not affect the monitor status.

Configuring Field Mapping for Ticket Samples

The ticket sample type is used for extracting events collected by external systems and importing them to Business Availability Center. When configuring an integration monitor's field mapping, select the **Tickets** sample type to load the tickets script. You can then copy the contents of the **Field Mapping** text box and paste it into a text editor to make your configuration changes. When you are done, copy the contents back into the Field Mapping text box.

This section includes the following topics:

- "Mandatory Values for the Ticket Script" on page 986
- "Optional Values for the Ticket Script" on page 987
- "Conditional Expression Example" on page 988
- "Ticket Script Example" on page 988

Mandatory Values for the Ticket Script

The tables below list mandatory and optional values for the ticket script.

Field Name	Type	Description	Example
time_stamp	DOUBLE	Time stamp in seconds since Jan 1 1970	time_stamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS").
severity	INT	Can be one of the following preconfigured severities (based on applicable integer): SEVERITY_UNKNOWN SEVERITY_INFORMATIONAL SEVERITY_WARNING SEVERITY_MINOR SEVERITY_MAJOR SEVERITY_CRITICAL	4".equals($severity) ? "Low" : ("3".equals($severity) ? "Average" : ("2".equals($severity) ? "High" : ("1".equals($severity) ? "Critical" : "Unknown")))
target_name	STRING	Name of the entity (usually a service) that generated the ticket.	target_name=”mail service” (Do not enter static string here, should be retrieved dynamically from the ticket.)
data_source	STRING	System that generated the ticket	data_source=”ticketing” (This string should not be edited for HP ServiceCenter integration and must be edited for a generic technology integration monitor.)
ticket_id	STRING	ID of the ticket	ticket_id=112233
ticket_state	STRING	One of the states in the incident lifecycle as defined in the ticketing system.	"Open" / "Closed"

Field Name	Type	Description	Example
ticket_type	STRING	Type of the incident as defined in the ticketing system.	"Incident"
orig_severity_name	STRING	Severity in external EMS terminology	orig_severity_name ="Cleared"

Optional Values for the Ticket Script

The script includes comments describing the optional values available for the ticket script. They include those listed here:

Field Name	Type	Description	Example
subject	STRING	Middle/High level hierarchy describing the event source.	CPU, SAP application, hard disk
instance	STRING	Instance of subject that generated the event. The lowest level hierarchy describing the event source.	D:\\
object	STRING	Optional level in the hierarchy describing the ticket source	object="OS"
logical_group	STRING	Logical grouping of this ticket	logical_group=”error messages”
monitor_group	STRING	Monitor group that reported this ticket	monitor_group="log monitors on \\hostname"
elapsed_time	STRING	Elapsed time of the ticket.	
orig_severity_name	STRING	Severity name as defined in the ticketing system.	
attr1	STRING	Extra data slot	attr1=$history

Field Name	Type	Description	Example
attr2	STRING	Extra data slot	attr2=$moreHistory
attr3	STRING	Extra data slot	attr3="Design"
attr4	STRING	Extra data slot	attr4=$MonitorOutput
attr5	STRING	Extra data slot for long strings. Use for values up to 2000 chars.	attr5=$Longhistory

Conditional Expression Example

```
4".equals($severity) ? "Low" : ("3".equals($severity) ? "Average" :
("2".equals($severity) ? "High" : ("1".equals($severity) ? "Critical" : "Unknown")))
```

This example configures the severity of the ticket sample. It matches between the status terms used in the ticketing system to those used in Business Availability Center.

Ticket Script Example

```
[$DEFAULT_PARAMETERS$]
time_stamp:DOUBLE=$time_stamp
ticket_id=$ticket_id
ticket_state=$ticketStatus
severity:INT=$severity
target_name=$target_name
data_source="ticketing"
ticket_type="Incident"
orig_severity_name="4".equals($severity) ? "Low" : ("3".equals($severity) ? "Average" :
("2".equals($severity) ? "High" : ("1".equals($severity) ? "Critical" : "Unknown")))
```

Event Handler Structure

Each event handler has following structure:

```
[name]
Matching condition
Action directive
Tags
```

The names of **Matching condition**, **Action directive,** and additional directives start with dollar sign symbol (**$**). The names of tags should not start with dollar sign.

Comments are allowed in the field mapping. The comment starts with either **#**, **!**, or **;** character and continues to the end of the line.

This section includes the following topics:

- "Matching Condition" on page 990
- "Basic String Expressions" on page 994
- "Basic Conditional Expression" on page 994
- "Action Directive" on page 994
- "Tags" on page 995
- "Integration Monitor Field Mapping Examples" on page 996

Matching Condition

The Match Condition must be a valid boolean expression. The expression can contain calls to the operators and functions defined below. The expression can access the contents of the event that is being processed using the dollar sign ($) notation. For example, if the incoming event is SNMP Trap, then its enterprise OID can be accessed as $oid. For names specific to a monitor, refer to the documentation of the relevant monitor type.

The matching condition has the form:

```
$MATCH=Boolean expression
```

where the Boolean expression is one of the expressions listed in the table below. When mentioned in the description, the expression can also be used to assign values into tags (see “Tags” on page 995).

Expressions and Functions	Description	Examples	True if
<, <=, >, >=, ==, !=	Checks the numerical correctness of the expression. Can be used with INT or DOUBLE fields.	$MATCH= $numberOfLines == 100	$numberOfLines equals 100
		$MATCH= $numberOfColumns <= 107	$numberOfColumns equals 107 or less
equals(String)	Checks for string equality.	$MATCH= “ERROR”.equals($status)	$status equals the word ERROR
		$MATCH= $status.equals(“ERROR”)	$status equals the word ERROR
true, false	Constant Boolean values.	$MATCH= true	always true.

Expressions and Functions	Description	Examples	True if
&&, ||	To be used to combine any of the above boolean expressions.	$MATCH= $status.equals (“ERROR”) || $numberOfLines == 100	$status equals the word ERROR or if $numberOfLines equals 100
time()	Returns the current time, in seconds, since January 1, 1970 format. Can be used with DOUBLE fields.	$MATCH= $timeStampField > (time()-600)	the value of the $timeStampField is newer then ten minutes ago (in seconds, since January 1, 1970 format)
parseInt (String), parseDouble(String),	Use to convert strings to numeric values. The input string should be a valid representation of an integer or a floating point number. **Note:** calling this function on a string that cannot be interpreted as a number causes an error and the incoming event is dropped. Can also be used with INT or DOUBLE fields.	$MATCH= parseInt($size) > 10	the string value in $size is an integer larger than 10.

Expressions and Functions	Description	Examples	True if
str_to_ seconds(Str1, Str2)	Calculates the timestamp (in seconds, since January 1, 1970 format) held in the first String using the format in the second string. Can also be used with DOUBLE fields.	$MATCH= str_to_seconds ($time,"yyyy-MM-dd HH:mm:ss.SSS") > time() **Note:** use the following symbols to represent time: Year - 'y' Month - 'M" Day of month - 'd' Hour - 'H' Minute - 'm' Second - 's'	the date specified in $time in yyyy-MM-dd HH:mm:ss.SSS format is later than the current time. For more information, search the Internet for SimpleDateFormat.
exist($field)	Checks for an existence of a field in the processed event and makes sure that it is not an empty value.	$MATCH= exist($status)	$status exists in the incoming event and is not an empty string.
isInt(String), isDouble (String)	Checks if the input string can be interpreted as an integer or a double number, respectively.	$MATCH=isDouble($size)	the string value in $size can be converted to a double.

Expressions and Functions	Description	Examples	True if
resolveHostIP (String hostname)	Performs DNS resolution from a server to its IP address. If the DNS resolution fails, the function returns the value unknown host.	target_ip= resolveHostIP ($host)	
resolveHostName (String hostname)	Performs DNS resolution from an IP address to a fully qualified domain name. If the DNS resolution fails, the function returns the originally input host name.	target_name= resolveHostName ($host)	

Any of the above expressions can be used and the expression can refer to incoming event fields. The value of the expression, which can be either **true** or **false**, determines whether the event handler is be used to process the event or not.

Basic String Expressions

The following table summarizes the string expressions that can be used in the field mapping:

Operation	Description	Examples
+	String concatenation	"trap type is " + $trap
substring	Substring of given string	$var4.substring(3,5)
indexOf	Return indexOf string in another string	$var4.indexOf($var3)

Basic Conditional Expression

One conditional expression is supported; the **?** operator. This operator can be used to compose three expressions into one (for example, <Conditional part> ? <if true part> : <if false part>).

Action Directive

The action directive has form:

$ACTION= TOPAZ_BUS_POST or DISCARD

The value of the Action directive defines whether the event is processed and forwarded to Business Availability Center, or discarded. This value takes effect only if the matching condition within the handler had been evaluated to positive value (that is, to **true**). The table below describes the effect of the different actions.

Action	Description	For Use With
TOPAZ_BUS_POST (event)	Send the event to the Business Availability Center bus and database.	HP Business Availability Center
TOPAZ_BUS_POST (ss_t)	Send the metrics to Application Management as SiteScope Data.	HP Business Availability Center
DISCARD	Do not send the data to HP Business Availability Center.	events you wish to filter out

Note: If you are using the metrics mapping, TOPAZ_BUS_POST(ss_t), the data is sent to the HP Business Availability Center database as SiteScope data, and thus saved to the database. For details on metrics mapping, see "Configuring Field Mapping for Measurement Samples" on page 982.

Tags

In addition to directives, the event handler contains **tags**. Each tag represents a field in the event that is forwarded to Business Availability Center. The tag's value can be evaluated when the event arrives to the integration monitor.

The general format of a tag is name[:type]=value.

The <name> is any string without spaces or dollar signs (**$**). The <type> specifies the type of field as reported to Business Availability Center. It can be either **INT**, **DOUBLE** or **STRING**. The default type is **STRING**.

By defining a tag, you can customize event forwarding to Business Availability Center. Thus getting more value from the external applications that generate those events. For example, if the monitor pulls out data from a database table column called AlertText, which contains a textual description of an alert, it is possible to send that data to Business Availability Center by adding the following line to an event handler section:

```
[event handler]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
text=$AlertText
```

Note: When adding tags, always add them after the **$MATCH** and **$ACTION**.

Integration Monitor Field Mapping Examples

Example 1: Universal Event Handler

```
[post them all]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL
szAlarmText:STRING=”post them all handler received an event”
```

Note that the **$MATCH** directive in the handler is set to **true**. This causes every event to match the handler and therefore every event is sent to the Business Availability Center Bus.

Example 2: Different Event Handlers for Different Severities

```
[Error Handler]
$MATCH= $status.equals(“ERROR”)
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_CRITICAL

[Info Handler]
$MATCH= $status.equals(“INFO”)
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL

[post them all]
$MATCH=true
$ACTION=TOPAZ_BUS_POST(event)
severity:INT=SEVERITY_INFORMATIONAL
```

In this example, an incoming event is matched against the **Error Handler** event handler. If the handler’s condition is true (that is, the value in the status field equals **ERROR**), then an event with a field called severity, whose value is **SEVERITY_CRITICAL**, is sent to HP Business Availability Center. An event can be matched only by a single handler. The first match stops the processing and therefore once an event is matched by a section, it is not processed by the next handler.

If the event was not matched by the first handler, the second handler comes into action and its match (which looks for status of **INFO**) is used to decide whether the second handler needs to take action. Finally, if the event does not match the second handler, the third universal handler is evaluated.

Note: Use only the mandatory and optional fields defined in the script templates when working with the field mapping. See the tables in the following sections for more information.

52

Integration SiteScope Monitors User Interface Settings

This chapter includes the pages and dialog boxes that enable you to add and edit integration SiteScope monitors.

HP OVO Event Monitor Settings

Description	The HP OVO Event Monitor allows you to integrate an existing HP OpenView installation with HP Business Availability Center by transferring HP OVO messages from HP OVO Server to an HP Business Availability Center server. This monitor supports: ➤ HP OVO 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 ➤ HP OVO versions 7.5 or later when installed on Windows Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"HP OVO Event Monitor" on page 917

The Add/Edit Integration HP OVO Event Monitor configuration file templates page includes the following areas:

Advanced Settings (Monitor Specific)

GUI Element	Description
Frequency	Set how often SiteScope attempts to execute the action defined for the monitor instance. Each monitor run updates the status of the monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days. **Default:** Monitor runs once every 10 minutes. **Minimum value:** 15 seconds
HP OVO Add-on TCP Port	Enter the TCP port number as configured in the HP OVO Integration Add-on. **Default value:** 9000
Fields Mapping	The out-of-the-box integration script that enables the monitor to correctly map the data it collects from the OVO installation to a format recognizable by the monitor and HP Business Availability Center. It is recommended to use the field mapping as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the file in the following location and edit it in your preferred text editor: **<SiteScope root directory>\conf\ems\hp\event.config**. To enable any changes, you must edit the monitor to reload the edited script. For details on the field mapping script template, see “Integration Monitor Field Mapping” on page 973.

Topology Settings

GUI Element	Description
Script	The out-of-the-box integration script that creates a topology in Business Availability Center that is based on the data collected from the OVO 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 OVO system and Business Availability Center's applications. It is recommended to 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: **<SiteScope root directory>/conf/ems/scripts/EMS_hpovo.py** and edit it in your preferred text editor. To enable any changes, you must edit the monitor to reload the edited script. For more details on editing the script, see "Topology Settings" on page 903.

HP ServiceCenter Monitor Settings

Description	This monitor enables you to integrate HP ServiceCenter incidents with HP Business Availability Center. The incidents in ServiceCenter are forwarded to Business Availability Center as samples by this SiteScope monitor. The samples are used in reporting data to the Business Availability Center applications, such as Service Level Management and Dashboard. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree. It is recommended to create a special group for the ServiceCenter integration.
Included in Tasks	"HP ServiceCenter Integration Workflow" on page 931
Useful Links	"HP ServiceCenter Monitor" on page 929

The Add/Edit Integration HP ServiceCenter Monitor settings page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Host	The server on which the HP ServiceCenter installation is running.
Port	The port designated for accessing HP ServiceCenter.
Username	The designated user name created in HP ServiceCenter for the purpose of this integration monitor.
Password	The password of the designated user created in HP ServiceCenter for the purpose of this integration monitor.

Advanced Settings (Monitor Specific)

GUI Element	Description
Fields Mapping	The out-of-the-box integration script that enables the monitor to correctly map the data it collects from the ServiceCenter installation to a format recognizable by the monitor and HP Business Availability Center. It is recommended to use the field mapping as is and it is not editable while creating the monitor. If you must customize the field mapping, locate the following file: **<SiteScope root directory>\conf\ems\peregrine\ticket.config** and edit it in your preferred text editor. To enable any changes, you must edit the monitor to reload the edited script. For details on the field mapping script template, see "Integration Monitor Field Mapping" on page 973.

GUI Element	Description
Test Script	Click to test the field mapping script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events are forwarded to Business Availability Center. You can also view the results of the test in the following log file: **<SiteScope root directory>/logs/bac_integration.log**. **Note:** The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.
Synch Flag	Select to enable the monitor to query ServiceCenter to retrieve all Incidents Changes from the time specified in the **Synch Time** setting. **Default**: Cleared **Note**: This flag is reset to cleared after each time the monitor retrieves the data from ServiceCenter.
Synch Time	Enter a value indicating the time from which the monitor retrieves incidents. Enter a value only when **Synch Flag** is selected.
Incident Management (probsummary table) query	Enter the text to add to the query that the monitor sends to ServiceCenter. You can add to the query to determine which Incidents the monitor retrieves. **Default**: type="bizservice" The query is set to retrieve only those incidents opened on CIs of type **bizservice**. **Note**: The syntax for the query must be specified by the ServiceCenter application. It is recommended that you consult the ServiceCenter help to create the text to add to the query and to test the query using the advanced search found in the ServiceCenter application.
Incident Open State	Indicates the initial state as defined in ServiceCenter for the incident lifecycle. **Default**: Open

Topology Settings

GUI Element	Description
Script	The out-of-the-box integration script that creates a topology in Business Availability Center that is based on the data collected from the ServiceCenter 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 ServiceCenter system and Business Availability Center's applications. It is recommended to 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: **<SiteScope root directory>/conf/ems/scripts/EMS_peregrine.py** and edit it in your preferred text editor. To enable any changes, you must edit the monitor for SiteScope to reload the edited script. For more details on editing the script, see "Topology Settings" on page 903.
Test Script	Click to test the topology script. This test gives you the results of what events are forwarded to Business Availability Center and what topology is mapped. You can also view the results of the test in the following log file: **<SiteScope root directory>/logs/bac_integration.log**. **Note**: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.

NetScout Event Monitor Settings

Description	The NetScout Event Monitor monitors alerts received from the NetScout nGenius server and forwards them to HP Business Availability Center. This provides a way to centralize data collection, display, and alerting for the conditions for which you might otherwise be unaware until something more serious happens. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"NetScout Event Monitor" on page 935

The Add/Edit NetScout Event Monitor page includes the following areas:

Advanced Settings (Monitor Specific)

GUI Element	Description
Frequency	Set how often SiteScope attempts to execute the action defined for the monitor instance. Each monitor run updates the status of the monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days. **Default**: Monitor runs once every 10 minutes. **Minimum value**: 15 seconds
Fields Mapping	The out-of-the-box integration script that enables the monitor to correctly map the data it collects from the NetScout installation to a format recognizable by the monitor and HP Business Availability Center. This script is not editable.
Run Alerts	Select the method for running alerts: ➤ If **for each event received from NetScout system** is chosen, then the monitor triggers alerts for every matching entry found. **Note:** If **for each event received from NetScout system** 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. ➤ If the **once, after all events from NetScout system were received** method is selected, then the monitor counts up the number of matches and triggers alerts based on the **Error if** and **Warning if** thresholds defined for the monitor in the Threshold Setting section.

GUI Element	Description
EMS Time Difference	Enter a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded. **Note**: 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.

Technology Database Integration Monitor Settings

Description	The Technology Database Integration Monitor allows you to collect event and time series data from database tables used by Enterprise Management Systems (EMS) by performing a query through a JDBC connection. The data retrieved is then processed and sent to HP Business Availability Center as samples (one sample for each row that was returned by an SQL query). Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Technology Database Integration Monitor" on page 939

The Add/Edit Technology Database Integration Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Database Connection URL	Enter a 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 test under the system DSN tab. Then, enter jdbc:odbc:test in this box as the connection URL. Alternatively, use the supplied MSSQL or Oracle driver to connect to the Database.
Database Driver	Enter the driver used to connect to the database. Use the Fully Qualified Class Name of the JDBC driver you are using.
SELECT	Enter the SELECT clause to be used in the SQL query. Enter ***** for all fields or a comma separated list of column names to be retrieved from the database. When specifying the SELECT clause, the column used as the enumerating field must appear in the clause.
FROM	Enter the FROM clause to be used in the SQL query. Enter a table name or a comma separated list of tables from which the selected columns should be extracted.
WHERE	Enter the WHERE clause to be used in the SQL query. This is an optional field which allows you to define the select criteria. Leaving it empty results in retrieving all the rows from the table defined in the FROM option.

<table>
<tr><th>GUI Element</th><th>Description</th></tr>
<tr><td><b>OS Integrated Security</b></td><td>Check this check box if you want to use the user name and password from Windows' user authentication to access the database. Entries in the Database Username and Database Password are ignored.
If this parameter is checked, you must use the DataDirect driver as your database driver.</td></tr>
<tr><td><b>Database User Name</b></td><td>Enter the user name used to login to the database.</td></tr>
<tr><td><b>Database Password</b></td><td>Enter a password used to login to the database.</td></tr>
<tr><td><b>Enumerating Field</b></td><td>Enter a name for a database field that can be used to order the events that are returned from the database query.
<b>Note:</b> The column used as enumerating field must be included in the SELECT clause.</td></tr>
<tr><td><b>Enumerating Field Type</b></td><td>Enter the type of field used to order the result set. This can be a DATE field, an INTEGER field, a DOUBLE floating point numeral field, or a LONG field.
The following table maps SQL types to the appropriate 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></td></tr>
</table>

GUI Element	Description
Initial Enumerating Value	Enter an initial value to be used as a condition for the initial run of this monitor instance. For example, if you specify the Enumerating Field Type as a field type DATE and you enter a value of 2000-31-01 12:00:00 in the **Start from** value field, only records that were added to the database after the specified date are forwarded. **Note:** The value of this field cannot be edited.
Sample Type	Select from the following sample types for this integration: ➤ **Events**. For details, see "Configuring Field Mapping for Event Samples" on page 976. ➤ **Measurements**. For details, see "Configuring Field Mapping for Measurement Samples" on page 982. ➤ **Tickets**. For details, see "Configuring Field Mapping for Ticket Samples" on page 985.
Load File	Click to load the script that is applicable to the sample type selected above.

GUI Element	Description
Field Mapping	The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring. The mapping itself is not editable in the UI. You must copy it into your preferred text editor, edit it, and then copy it back into this field. For details on the field mapping script template, see "Integration Monitor Field Mapping" on page 973.
Test Script	Click to test the field mapping script. It is highly recommended that you test the script before running the monitor. This test gives you the results in a separate window of what events or measurements are forwarded to Business Availability Center. You can also view the results of the test in the following log file: **<SiteScope root directory>/logs/bac_integration.log**. **Note**: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.

Advanced Settings (Monitor Specific)

GUI Element	Description
EMS Server Name	If you are reporting monitor data to an installation of HP Business Availability Center, enter a text identifier describing the database server that this monitor is monitoring. This text descriptor is used to identify the database server when the monitor data is viewed in an HP Business Availability Center report. 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.

GUI Element	Description
Max Rows	Specify the maximum number of rows the monitor retrieves from the database for each monitor cycle. **Default**: 5000 rows 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 value should be large enough 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 upon both monitor run frequency and network/system speed—is greater than, or equal to, the rate of data insertion on the monitored system.
EMS Time Difference	Enter a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded. **Note**: 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.

Topology Settings

GUI Element	Description
Select a Topology	Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propagates its status to the CIs mapped in this topology. Select from: ➤ **Custom**. You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the available topology. ➤ **Hosts**. Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the topology. ➤ **Hosts-Applications**. Creates a topology with an application CI and a host CI and an EMS monitor CI as the leaf node under each application CI and host CI. **Note**: It is recommended not to select **Custom** as this does not load a script and you must enter the entire script yourself. It is recommended to begin with either **Host** or **Host and Application** and edit one of those scripts. When editing the topology, you must ensure that an EMS Monitor CI is created as the leaf node to any CI that receives samples from the integration. For more details, see “Topology Settings” on page 903.
Load Script	Click to load the appropriate Jython script for the topology you selected in the **Select a Topology** option. If you selected **Custom**, there is no script to load.

GUI Element	Description
Script	The contents of the script are visible in this field. However, it is highly recommended not to edit the contents of the script here. You must copy the contents of the script into your preferred text editor, edit the script as needed, and then copy the contents back into this field. **Note**: The Jython script is very sensitive to spaces and tabs. For more details on editing the script, see "Topology Settings" on page 903.
Test Script	Click to test the topology script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is created. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period. You can also view the results of the test in the following log file: **<SiteScope root directory>/logs/bac_integration.log**. **Note**: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.

Technology Log File Integration Monitor Settings

Description	Technology Log File Integration Monitor watches for specific entries added to a log file of a Enterprise Management System (EMS) application by trying to match against a regular expression. From each matched entry, one sample is created and sent to HP Business Availability Center. Each time the monitor runs, it examines log entries added since the last time it ran. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Technology Log File Integration Monitor" on page 947

The Add/Edit Technology Log File Integration Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
Frequency	Select how often the Technology Log File Integration Monitor checks the log file for data to forward to HP Business Availability Center. **Default value:** 10 minutes Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. **Note:** ➤ The update interval must be a minimum of 15 seconds or longer. ➤ It is possible to define a monitor with zero frequency. However this monitor runs only if activated manually or according to the frequency of the composite or e-business transaction monitor including it.
Servers	Choose the server where the log file you want to monitor is located. Use the drop-down list to select a server from the list of UNIX remote servers that are available to SiteScope.

GUI Element	Description
Log File Pathname	Enter the path to the log file you want to extract data from. ➤ **Remote UNIX.** For reading log files on remote UNIX machines, the path must be relative to the home directory of UNIX user account being used to login to the remote machine. Select **Preferences** > **UNIX Servers** for information on which UNIX user account is being used. ➤ **Remote Windows NT/2000 through NetBIOS.** You can also monitor log files by including the UNC path to the remote log file. For example, \\remoteserver\sharedfolder\filename.log. 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 via the operating system is unsuccessful, SiteScope tries to match the \\remoteserver with servers currently defined as remote NT connection profiles (displayed in the Windows Remote Preferences servers list). If an exact match is found for \\remoteserver in the remote NT connection profiles, SiteScope tries to use this connection profile to access the remote log file. If no matching server name is found, the monitor reports that the remote log file can not be found. ➤ **Remote NT through SSH.** You need to select the remote server using the **Server** selection above. It is not necessary to select a remote Windows server if you are using NetBIOS to connect to remote Windows servers. Optionally, you can use a regular expression to insert date and time variables. For example, you can use a syntax of s/ex$shortYear$$0month$$0day$.log/ to match date-coded IIS log file names.

GUI Element	Description
Content Match	Enter the text to look for in the log entries. You can also use regular expression in this entry to match text patterns. Unlike the content match feature of other SiteScope monitors, the Log File Monitor content match is run repeatedly against the most recent content of target log file until all matches are found. This means the monitor not only reports if the match was found but also how many times the matched pattern was found. To match text that includes more than one line of text, add an **s** search modifier to the end of the regular expression.
Sample Type	Select from the following sample types for this integration: ➤ **Events**. For details, see "Configuring Field Mapping for Event Samples" on page 976. ➤ **Measurements**. For details, see "Configuring Field Mapping for Measurement Samples" on page 982. ➤ **Tickets**. For details, see "Configuring Field Mapping for Ticket Samples" on page 985.
Load File	Click to load the script that is applicable to the sample type selected above.
Field Mapping	The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring. The mapping itself is not editable in the UI. You must copy it into your preferred text editor, edit it, and then copy it back into this field. For details on the field mapping script template, see "Integration Monitor Field Mapping" on page 973.

GUI Element	Description
Test Script	Click to test the field mapping script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period. You can also view the results of the test in the following log file: **<SiteScope root directory>/logs/bac_integration.log**. **Note**: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.

Advanced Settings (Monitor Specific)

GUI Element	Description
No Error if File Not Found	Select this box if you want this monitor to remain in good status, if the file is not found.
Log File Encoding	If you are reading a log file whose encoding is different than the SiteScope machine's default encoding, specify the log file encoding.

GUI Element	Description
Run Alerts	Select the method for running alerts for this monitor: ➤ Select **for each log entry matched** to have the monitor trigger alerts for each and every matching entry found regardless of the defined threshold settings and the monitor status (good, warning, or error). **Note:** 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 even if the target log file is not found. The monitor triggers alerts if one or more matching entries are found and the Error if or Warning if thresholds are defined accordingly in the Advanced Options section (for example, setting Error if to the default of matchCount > 0). ➤ Select **once**, **after all log entries have been checked** to have the monitor count up the number of matches and trigger alerts one time based on the **Error if** and **Warning if** thresholds defined for the monitor in the Advanced Options section. **Note:** 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 <matchDetails> 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 e-mail alerts or other alert types that work with template properties. E-mail alert templates are stored in the <SiteScope root directory>\templates.mail directory.

GUI Element	Description
EMS Time Difference	Enter a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded. You can also view the results of the test in the following log file: **<SiteScope root directory>/logs/bac_integration.log**. **Note**: 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.

Topology Settings

GUI Element	Description
Select a Topology	Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propogates its status to the CIs mapped in this topology. Select from: ➤ **Custom**. You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or EMS monitor CIs. ➤ **Hosts.** Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the typology. ➤ **Hosts-Applications.** Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI as leaf nodes of the application CI. The host CI also has an EMS monitor CI as a leaf node. **Note**: It is recommended not to select **Custom** as this does not load a script and you must enter the entire script yourself. It is recommended to begin with either **Host** or **Host and Application** and edit one of those scripts. For more details, see “Topology Settings” on page 903.
Load Script	Click to load the appropriate Jython script for the topology you selected in the **Select a Topology** option. If you selected **Custom**, there is no script to load.

GUI Element	Description
Script	The contents of the script are visible in this field. However, it is highly recommended not to edit the contents of the script here. You must copy the contents of the script into your preferred text edit, edit the script as needed, and then copy the contents back into this field. **Note**: The Jython script is very sensitive to spaces and tabs. For more details on editing the script, see "Topology Settings" on page 903.
Test Script	Click to test the topology script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is mapped. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period. You can also view the results of the test in the following log file: <**SiteScope root directory>/logs/bac_integration.log**. **Note**: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.

Technology SNMP Trap Integration Monitor Settings

Description	The Technology SNMP Trap Integration Monitor watches for SNMP traps received by SiteScope from third-party Enterprise Management Systems (EMS). For each SNMP trap that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the SNMP trap values. The third-party EMS systems need to be configured to send traps to the SiteScope server. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Technology SNMP Trap Integration Monitor" on page 955

The Add/Edit Technology SNMP Trap Integration Monitor page includes the following areas:

Advanced Settings (Monitor Specific)

GUI Element	Description
Frequency	Set how often SiteScope attempts to execute the action defined for the monitor instance. Each monitor run updates the status of the monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days. Default: Monitor runs once every 10 minutes. Minimum value: 15 seconds

GUI Element	Description
Sample Type	Select from the following sample types for this integration: ➤ **Events**. For details, see "Configuring Field Mapping for Event Samples" on page 976. ➤ **Measurements**. For details, see "Configuring Field Mapping for Measurement Samples" on page 982. ➤ **Tickets**. For details, see "Configuring Field Mapping for Ticket Samples" on page 985.
Load File	Click to load the script that is applicable to the sample type selected above.
Field Mapping	The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring. The mapping itself is not editable in the UI. You must copy it into your preferred text editor, edit it, and then copy it back into this field. For details on the field mapping script template, see "Integration Monitor Field Mapping" on page 973.
Test Script	Click to test the field mapping script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period. You can also view the results of the test in the following log file: <**SiteScope root directory**>**/logs/bac_integration.log**. **Note**: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.

GUI Element	Description
Run Alerts	Choose the method for running alerts: ➤ If **for each SNMP Trap received from EMS system** is chosen, then the monitor triggers alerts for every matching entry found. When the Technology SNMP Trap Integration Monitor is run in the for each SNMP Trap received from EMS system alert method, the monitor never reports a status of error or warning, regardless of the results of the content match or even if the target SNMP Trap is not found. ➤ If **once, after all SNMP Traps from EMS system were received** is chosen, then the monitor counts up the number of matches and triggers alerts based on the Error If and Warning If thresholds defined for the monitor in the Advanced Settings section.
EMS Time Difference	Enter a value to account for any time differences greater than one minute between the system clock time on the monitored EMS machine and the server where SiteScope is running. This is only needed when the monitored data includes time data and the data shows a difference between the EMS machine and the SiteScope server. If the time difference is too great, the data may be discarded. **Note**: 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.

Topology Settings

GUI Element	Description
Select a Topology	Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propogates its status to the CIs mapped in this topology. Select from: ➤ **Custom**. You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or EMS monitor CIs. ➤ **Hosts.** Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the typology. ➤ **Hosts-Applications.** Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI as leaf nodes of the application CI. The host CI also has an EMS monitor CI as a leaf node. **Note**: It is recommended not to select **Custom** as this does not load a script and you must enter the entire script yourself. It is recommended to begin with either **Host** or **Host and Application** and edit one of those scripts. For more details, see "Topology Settings" on page 903.
Load Script	Click to load the appropriate Jython script for the topology you selected in the **Select a Topology** option. If you selected **Custom**, there is no script to load.

GUI Element	Description
Script	The contents of the script are visible in this field. However, it is highly recommended not to edit the contents of the script here. You must copy the contents of the script into your preferred text edit, edit the script as needed, and then copy the contents back into this field. **Note**: The Jython script is very sensitive to spaces and tabs. For more details on editing the script, see "Topology Settings" on page 903.
Test Script	Click to test the topology script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is mapped. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period. You can also view the results of the test in the following log file: <**SiteScope root directory**>**/logs/bac_integration.log**. **Note**: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.

Technology Web Service Integration Monitor Settings

Description	The Technology Web Service Integration Monitor enables a Web service entry point to SiteScope. The monitor can be used to report data from third-party Enterprise Management Systems (EMS) to SiteScope through Web service. Both event and metrics entry points into HP Business Availability Center are published for external systems to use. For each event and/or metric that SiteScope receives, a sample is forwarded to HP Business Availability Center containing the event and/or metrics values. Use this page to add the monitor or edit the monitor's properties. **To access:** ➤ In the monitor tree, right-click a group and select **Add Monitor.** ➤ In the Contents tab for the group, click **Add Monitor**.
Important Information	Monitors must be created in a group in the monitor tree.
Useful Links	"Technology Web Service Integration Monitor" on page 963

The Add/Edit Technology Web Service Integration Monitor page includes the following areas:

Main Settings (Monitor Specific)

GUI Element	Description
System ID	Enter a text system id for the Technology Web Service Integration Monitor instance. Each received message from the EMS system holds a system id. Each monitor receives messages only with a system id that matches the system id defined in the monitor. The system id is unique for all monitors. Enter the system id that represents the messages that you want this monitor to receive.

GUI Element	Description
Sample Type	Select from the following sample types for this integration: ➤ **Events**. For details, see "Configuring Field Mapping for Event Samples" on page 976. ➤ **Measurements**. For details, see "Configuring Field Mapping for Measurement Samples" on page 982. ➤ **Tickets**. For details, see "Configuring Field Mapping for Ticket Samples" on page 985.
Load File	Click to load the script that is applicable to the sample type selected above.
Field Mapping	The monitor uses the field mapping script to correctly map the data it collects from the monitored application to a format recognizable by HP Business Availability Center. To enable the integration, you must configure these mappings as required by the environment you are monitoring. The mapping itself is not editable in the UI. You must copy it into your preferred text editor, edit it, and then copy it back into this field. For details on the field mapping script template, see "Integration Monitor Field Mapping" on page 973.
Test Script	Click to test the field mapping script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period. You can also view the results of the test in the following log file: <**SiteScope root directory**>**/logs/bac_integration.log**. **Note**: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.

Advanced Settings (Monitor Specific)

GUI Element	Description
Frequency	Select how often the monitor should update its status. The **Frequency** setting for the monitor controls only the status reports. The Web transaction is forwarded when it is received without any delay. Use the drop-down list to the right of the text box to specify an update interval in increments of seconds, minutes, hours, or days. **Default value:** 10 minutes **Note:** ➤ The interval must be a minimum of 15 seconds or longer. ➤ It is possible to define a monitor with zero frequency. However this monitor runs only if activated manually or according to the frequency of the composite or e-business transaction monitor including it.

Topology Settings

GUI Element	Description
Select a Topology	Select a Jython script to create the topology in Business Availability Center for the samples retrieved from the monitored application. The monitor propogates its status to the CIs mapped in this topology. Select from: ➤ **Custom**. You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard host or EMS monitor CIs. ➤ **Hosts.** Creates a host CI with an EMS monitor CI as a leaf node. The EMS monitor CI is the lower level node within the typology. ➤ **Hosts-Applications.** Creates a topology with an application CI as the parent CI and a host CI and EMS monitor CI as leaf nodes of the application CI. The host CI also has an EMS monitor CI as a leaf node. **Note**: It is recommended not to select **Custom** as this does not load a script and you must enter the entire script yourself. It is recommended to begin with either **Host** or **Host and Application** and edit one of those scripts. For more details, see “Topology Settings” on page 903.
Load Script	Click to load the appropriate Jython script for the topology you selected in the **Select a Topology** option. If you selected **Custom**, there is no script to load.

GUI Element	Description
Script	The contents of the script are visible in this field. However, it is highly recommended not to edit the contents of the script here. You must copy the contents of the script into your preferred text edit, edit the script as needed, and then copy the contents back into this field. **Note**: The Jython script is very sensitive to spaces and tabs. For more details on editing the script, see "Topology Settings" on page 903.
Test Script	Click to test the topology script. It is highly recommended that you test the script before running the monitor. This test gives you the results of what events or measurements are forwarded to Business Availability Center and what topology is mapped. The test relies on an open socket connection for several minutes and then displays what data was captured for the test period. You can also view the results of the test in the following log file: **<SiteScope root directory>/logs/bac_integration.log**. **Note**: The test does not forward samples to Business Availability Center; it tests that the configuration is correct and that data is forwarded accurately when the monitor does run.

Part VI

Templates

53

Using SiteScope Templates

The templates feature enables you to deploy standardized group and monitor configurations across multiple infrastructure elements with a minimal number of configuration steps.

About SiteScope Templates

Many business system environments consist of a large number of similar or redundant elements. Standardization of hardware and software facilitates system management. Monitoring the availability of these systems generally requires duplicated sets of monitors including more than one type of monitor. For example, if there are 50 servers in the infrastructure, the same key system resources, such as CPU, disk space, and memory, can be monitored for each server even though the applications that are running on each server may be different. Templates help speed the deployment of monitors across the enterprise through standardization of group structures, monitor types and configuration settings.

You create templates within a template container in the monitor tree. These elements are then displayed in the monitor tree where you can access them for changes or deployment. For more information, see "Understanding Templates" on page 1041.

You use templates to deploy a standardized pattern of monitoring to multiple elements in your infrastructure. Effective development and use of templates requires some planning. For more information, see "Planning Templates" on page 1045.

You create a template by adding and configuring groups, servers, monitors, alerts, and variables to the template using actions similar to adding these elements to the monitor tree.

You use template variables as substitution markers for configuration settings that you want to change dynamically or interactively each time you deploy the template. Creating and referencing variables is an action that is unique to templates. Template variables use a special syntax. For more information, see "Working with Template Variables" on page 1057.

Several SiteScope monitor types use a measurement counter browser feature to dynamically query applications and systems for the metrics that are available for monitoring. When you create one of these monitors manually, you use a multiple step procedure to view and select counters. An alternative method is used to select counters when deploying templates. For more information, see "Counter Selection in Monitor Templates" on page 1062.

After you create and configure templates, you deploy them by using the monitor tree, right-click menus. You deploy templates using actions similar to copying and pasting monitor groups and monitors in the SiteScope hierarchy. For more information, see "Using Templates to Deploy SiteScope Monitoring" on page 1069.

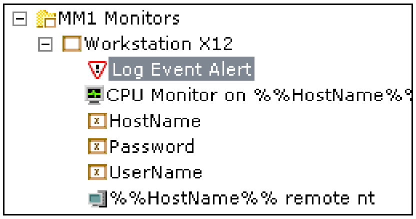
Understanding Templates

Templates are objects you use to reproduce servers, monitors, and alerts according to a predefined pattern and configuration. Templates include group, server, monitor, and alert template objects as placeholders representing the type and configuration of corresponding items that you want to deploy in your monitoring environment. You can then deploy all of the items defined in the template in a single operation by copying the template to a location in the SiteScope hierarchy. Templates also use template variables that you use to interactively set certain monitor, server and alert configuration settings when you deploy the template.

You can create as many templates as you need. Once you have created a template, you can use it to deploy monitors as often as needed.

If SiteScope monitoring has not yet been configured and you are not familiar working with SiteScope monitors and groups, it is recommended that you set up some sample groups, monitors, and alerts before you create templates. This helps familiarize you with the monitor configurations and the relationship between monitors, groups, and alerts.

The following is an example of the monitor tree showing a template container and a single template. The container labeled **MM1 Monitors** is expanded to display the template **Workstation X12** that contains a template alert, a template monitor, three template variables, and a template remote server.



```
⊟ MM1 Monitors
   ⊟ Workstation X12
        Log Event Alert
        CPU Monitor on %%HostName%
        HostName
        Password
        UserName
        %%HostName%% remote nt
```

Template Objects

Templates are created and stored in a template container in the monitor tree. The template variable definitions and SiteScope objects configurable using the template are displayed as objects within the template. The following table describes the objects used in templates.

The following table describes the existing template objects:

Icon	Object Type	Description	Possible Contents
	Template Container	You use a template container to store and manage one or more templates. Template containers allow you to group and organize multiple templates in ways that describe their purpose or classification. Template containers are added only to the SiteScope node.	Templates
	Template Group	You use template groups to replicate monitoring deployment to multiple locations in the infrastructure.	➤ Template Monitors ➤ Template Alerts ➤ Groups

Icon	Object Type	Description	Possible Contents
□	Template	An individual template is comprised of the object definitions of those objects that are created when the template is deployed. You can add a template only to a template container node within the monitor tree.	➤ Template Monitors ➤ Template Servers ➤ Template Alerts ➤ Template Variables ➤ Groups
x	Template Variable	A variable is used to enable prompting for user input during template deployment. Template variables are either user defined or pre-defined system variables that provides access to the list of remote server connections known to SiteScope.	None
🖥	Template Remote Server	Template remote servers are used to define remote servers preferences that are created when the template is deployed. These can be either UNIX or Windows servers. Template servers can only be added to templates.	None

Icon	Object Type	Description	Possible Contents
🖥	Template Monitor	Template monitors are used to define monitors that are created when the template is deployed. Template monitors may be added to templates or to template groups.	Template Alerts
⚠	Template Alert	Template alerts are used to define alerts on monitors that are created when the template is deployed. Template alerts may be added to templates, template groups, or template monitors. Template alerts are enabled for all the monitors belonging to the object for which they were defined. For example, if an alert is defined for a monitor, then it is activated on that monitor only. If an alert is defined for a template, then it is activated for all the monitors in the template.	None

There are two ways to perform actions on a template object. Each template object has a right-click action menu that you can use to add, edit, or delete objects from it. In addition, when you select the template object in the monitor tree, a dialog box is displayed in the Content page where you can perform various actions on it.

Template monitors are not active monitor instances. Monitors are created and activated based on these template configurations when you actually deploy the template.

Template Remote Servers

When using remote servers in templates, it is not possible to set the server using a regular variable (%%variable_name%%).

- If the remote servers are already defined, use the $$SERVER_LIST$$ variable. For details, see "Syntax for System Variables" on page 1059.
- If the remote servers are not defined, you can use the template remotes for Windows or UNIX and enter the remote name in the server field or optionally, you can create variables for the remotes and reference the variable in the template remote. For details, see "Template Remotes" on page 1053.

Planning Templates

Template planning is important for effective SiteScope management. You should consider the group and monitor relationships and properties in the template structure and how it fits into the overall monitoring environment. The following are things to consider as you plan templates:

- **Variable properties.** Decide which monitor configuration properties vary from one template deployment to another. For example, the target server address or resource to be monitored is a common variable property. You should also consider what naming conventions you want to use for groups and monitors. You use template variables to enter or select values for variable properties each time you deploy the template. Not all monitor configuration properties can be configured using variables. For more information, see "Working with Template Variables" on page 1057.
- **Servers.** Decide which servers are the target servers, where the objects monitored are located. Template servers are replicated automatically when the template is deployed. You can also define them manually in the Windows Remote Preferences or UNIX Remote Preferences section of the monitor tree.

- **Monitor types.** Decide which monitor types you want to replicate using templates. These should be monitor types that monitor multiple systems. For example, CPU, Disk, Memory and Service monitor types are commonly deployed for each server in the infrastructure. You can also include multiple instances of the Service Monitor type in a template to monitor different services or processes running on each server.
- **Common properties.** For configuration properties that should be the same from one template deployment to another, you need to decide what the values should be. For example, the **Frequency** setting is a required setting for each monitor type. The default setting is 10 minutes. Depending on what is to be monitored and the overall monitor load, you may want to change this value so that monitors created by using the template run more often.
- **Group structure.** Decide the group structure you want to use to organize the monitors. The organization groups and monitors in the template should be compatible with your overall plan for organizing the monitoring in your environment. The group structure you use may impact reporting, alerting, and monitoring.
- **Alerts.** Decide if you want to deploy alerts as part of the template. Consider which alert types and actions you want to associate with the templates and monitors. Alerts deployed as part of a template have their **Alert Targets** property set to all monitors defined in the template. For example, a template alert added to a template group alerts on any monitor belonging to that group. If this does not fit your alerting plan, you need to edit the alert configuration after deployment or add alerts manually.

Creating Templates

The steps for creating SiteScope templates are similar to the steps you use to create other objects in SiteScope. The following sections describe the steps you use to create the objects used for templates:

- "Creating Template Containers and Templates" on page 1047
- "Configuring Templates" on page 1048

Creating Template Containers and Templates

All templates for creating monitors, groups, and alerts are stored in a template container. Template containers can be added only to the SiteScope node in the monitor tree.

You can create multiple templates under a single template container. Before creating template variables and configuring servers, monitors, groups, or alerts for the template, you must create a template object (container or group) in the monitor tree to store the configurations and associated variables.

To create a template container:

1. Right-click the SiteScope node in the tree. The SiteScope action menu opens.
2. Select **New Template Container**. The New Template Container window opens in the content area.
3. Enter a name for the template container in the **Name** text box. Maximum length: 250 characters.
4. Optionally, if there are any categories defined in this enterprise, you can assign a category to the template container under the **Category Settings** section.

   For details on defining categories, see "Working with Categories" on page 173.
5. Optionally, you can assign a description to the template container under the **Advanced Settings** section. The description is displayed in the Contents tab for the SiteScope node.
6. Click **Add** to create the template container.

   After you create a template container object you use the following steps to add a template object to the container. The template is the object into which you add or create monitor and group configuration objects.

To create a template:

1. Select a template container in the monitor tree. The Template Container Actions dialog box is displayed.

   Alternatively, right-click a template container in the monitor tree. The Templates action menu is displayed.

2. Select **New Template** to display the New Template window in the Content page.

3. Enter a name for the template in the **Name** text box.

4. Optionally, if there are any categories defined in this enterprise, you can assign a category to the template under the **Category Settings** section.

   For details on defining categories, see “Working with Categories” on page 173.

5. Optionally, if there are any advanced settings defined in this enterprise, you can assign a description of the object to the template container under the **Advanced Settings** section. The description appears only when editing or viewing the object properties.

6. Click **OK** to create the template. The name you entered appears in the monitor tree as a child node to the templates container.

Configuring Templates

The two methods for adding configurations to the created template are:

- Copy an existing group and monitor hierarchy from a SiteScope to the template and edit the elements for use as a template. This method is described below.
- Manually enter the configurations you want to include in the template. For details, see “Manually Creating Template Configurations” on page 1049.

Tip: If the SiteScope includes standardized monitoring examples, it may be easiest to copy that pattern from the SiteScope and convert the configurations to a template.

Copying Existing Configurations to a Template

Once you have created a template container, template, and template variables, you can copy monitors and alerts that you have already configured to the template. Use the following steps to create template elements by copying groups, monitors or alerts from an existing SiteScope container.

To copy existing SiteScope elements to a template:

1. Expand the SiteScope node and group nodes as necessary to locate the configurations you want to copy to the template.
2. Right-click the selected group, monitor, or alert. The object's action menu opens.
3. Choose **Copy** from the menu.
4. Right-click the template or group within the template folder to which you want to add the copied configurations. The template action menu opens.
5. Choose **Paste**. The copied element is added to the template as a child of the selected element.
6. If you are using template variables in the new template, edit each copied object by right-clicking the object and choosing **Edit** to replace the applicable configuration field's value with the appropriate variable syntax. For details, see "Referencing Template Variables" on page 1061.

Manually Creating Template Configurations

If there are no applicable SiteScope monitor elements in your enterprise or if you want to create new objects or settings, you can create templates manually. You do this by creating template groups, monitors, servers, and alerts.

You can create the following objects in a template. It is recommended to create these objects in the order listed, although you may not always require all of the objects.

- "Template Groups" on page 1050
- "Template Variables" on page 1051
- "Template Remotes" on page 1053

- “Template Monitors” on page 1055
- “Template Alerts” on page 1056

Template Groups

If you want the template to be divided into groups, start by creating a group within the template. This step is optional.

You can add groups to templates or to template groups to create subgroups.

Note: The following procedure creates a group to which you can add one or more monitors, alerts, or subgroups. You can also create a template containing multiple monitors and alerts that are not contained within a group. Such a template can only be deployed to an existing SiteScope group container and not directly to the SiteScope node.

To create a group within a template:

1. Select a template or a template group in the monitor tree. The Template Actions or Template Group Actions dialog box opens.

   Alternatively, right-click a template or a template group in the monitor tree. The Template or Template Group actions menu opens.

2. Select **New Group**. The New Template Group window opens.

3. Enter a name for this group in the **Group Name** text box. You can use a template variable in the **Group Name** text box, enabling you to specify a different name for the group every time that you deploy the template. For details, see step “Referencing Template Variables” on page 1061.

4. Enter optional group settings in the **Advanced Settings** section. For details on configuring group settings, see “Manage SiteScope Monitor Groups” on page 374.

5 Optionally, if there are any categories defined in this enterprise, you can assign a category to the template under the **Category Settings** section.

For details on defining categories, see “Working with Categories” on page 173.

6 Click **OK** to save your settings and add the group to the template.

Template Variables

The first objects that you typically want to create in a template are variables, because these are referred to when you create monitors, servers, and alerts.

Template variables can only be added to a template and not to a template container or any other type of template object, such as a template monitor, template group, or template remote server.

For details, see “Working with Template Variables” on page 1057.

To add a variable to a template:

1 Select a template in the monitor tree. The Template Actions dialog box opens.

Alternatively, right-click a template. The Template actions menu opens.

2 Select **New Variable.** The New Template Variable dialog box opens.

3 Enter a variable name in the **Name** text box. This name is used to identify the variable in the template in the monitor tree. This is the name that must be used when referring to the variable in other template objects. For details, see “Working with Template Variables” on page 1057.

Note: The name of a variable cannot be edited once the variable has been added. To change a variable name, delete the variable and create a new one with the correct name.

4 If you want a different name to be displayed instead of the variable name upon deployment, enter a display name in the **Display Name** box. You should still use the variable name when referencing the variable in a template object.

5 Enter a text description in the **Description** text box. When the template is deployed, this description is displayed along with an entry field when you click the **Show Description** button in the upper-right side of the page.

6 Optionally, enter a default value in the **Default Value** text box to be used for this variable substitution. If you do not enter a value in this field and the field requires a value, you are prompted to enter a value when deploying the template.

7 Optionally, you can enter the variable display sequence number in the **Display Order in Template** box. This is the order in which SiteScope prompts you to enter values for a variable upon deployment. Variables are displayed in ascending order. Variables that have no display number are displayed at the end.

Note: The display order does not change the order of the variables within the template definition.

8 By default, the variable field requires a value and prompts you to enter a value when deploying the template. To set a variable with a non-mandatory value, clear the **Mandatory Variable** check box. When this option is cleared, SiteScope uses an empty String("") as a value for a non-mandatory variable.

Note: SiteScope validates places that are referenced with non-mandatory variables and displays an error if it finds a non-mandatory variable has been configured and is referenced in a place where a string is required.

9 Click **OK** to add the variable to the template.

For more information about variables, see "Working with Template Variables" on page 1057.

Template Remotes

You can create template remote servers in the template. These servers are added to the monitor tree under Windows Remote Preferences or UNIX Remote Preferences when the template is deployed. For details on remote preferences, see “Windows Remote Preferences Overview” on page 195 and “UNIX Remote Preferences Overview” on page 201.

You can use remote servers in templates by defining a template remote as follows:

- Add a template remote to the template (right-click a **Template** object and click **New Remote NT** for Windows or **New Remote Unix**) referencing the variable.
- Create at least one template monitor and use the same name exactly in the **Server** field as used for the template remote.
- Optionally, create a variable (right-click a **Template** object and click **New Variable**) that represents the remote servers. If you create a variable, the remote template must reference this variable in the **Host** field.

  This enables you to add each server as you deploy the template when asked to enter the required information for the variables. Each time you enter a server name for the variable, a monitor instance is created for that server and the server is added to remote preferences. The server is added to Remote Preferences only if the server did not already exist as a remote preference.

Note: If the remote servers onto which you want to deploy monitor templates already exist under Remote Preferences, you can reference these servers within the monitor template. You do this by referencing the system variable $$SERVER_LIST$$ which identifies the servers accessible to the SiteScope. For details, see “Variable Syntax” on page 1058.

Template servers can only be added to a template and not to a template container or any other type of template object, such as a template monitor or alert.

To add a remote server to a template:

1 Select a template in the monitor tree. The Template Actions dialog box opens.

Alternatively, right-click a template in the monitor tree. The Template actions menu opens.

2 Select either the **New Remote NT** (for a Windows server) or the **New Remote Unix** (for a UNIX server) option. The New Template NT Remote window or the New Template UNIX Remote window opens.

Note: The following operating systems are supported when defining Remote UNIX servers: AIX, FreeBSD, HP, HP64, Linux, MacOSX, OPENSERVER, RHESlinux, SCO, SGI, Sun, Tru64, Tru64 4.x.

3 Enter the host string in the **Host** text box.

Note: The **Host** field must match an actual server host name after values are substituted for the variables at the time that the template is deployed. If the **Host** field does not match a server name at that time, the monitor fails.

4 Enter the actual values for those fields that remain constant throughout the template deployment.

5 Enter a name for the new template variable in the **Name** field.

Note: Names must be unique, otherwise the deployment fails.

6 Enter template variables in those fields whose values are replaced with a variable value when the template is deployed. For details, see "Referencing Template Variables" on page 1061.

7 Optionally, if there are any categories defined in this enterprise, you can assign a category to the template container under the **Category Settings** section.

For details on defining categories, refer to “Working with Categories” on page 173.

8. Optionally, you can set various parameters under the **Advanced Settings** section. For details, see “Windows Remote Preferences Overview” on page 195 or “Log Preferences” on page 250.
9. Click **OK** to save your settings and add the server to the template.

Template Monitors

After you have created variables and servers in the template, you may create the monitor templates. These are used as the basis for the creation of actual monitors at the time that the template is deployed.

To add a monitor to a template:

1. Select the template or the template group. The Template Actions dialog box opens.

   Alternatively, right-click the template or the template group. The Template action menu opens.
2. Select **New Monitor.** The New Monitor window opens.
3. Select the monitor type you want to configure for the template. The New Monitor window for that monitor type opens.
4. Enter a monitor name of your choosing in the **Name** text box. The monitor name may contain template variables.
5. Enter the host name in the **Servers** text box. This can be an actual value or it can be comprised of variables and text strings.

Note: A template monitor may run on servers that are defined by template servers at the time of template deployment. Alternatively, they may run on servers defined manually in the Remote Preferences branch of the monitor tree.

Whichever is the case, the value in the **Servers** field must match the host name of an actual server at the time that the template is deployed and after values have been substituted for the template variables. If the server name does not match the host name of a real server, the monitor fails.

6 Enter the frequency with which the monitor runs in the **Frequency** text box.

7 Enter values as required in the Advanced Settings, Threshold Settings, Custom Properties, HP BAC Logging, and Category Settings sections. For details on configuring SiteScope monitors, see “Working with SiteScope Monitors” on page 383.

8 Click **OK** to save the configuration and add the monitor configuration to the template group.

Template Alerts

Alerts can be added to a template group if the alert is to be activated for all monitors in the group or it can be added to an individual template monitor.

To add an alert to a template:

1 Click either a template monitor or group. The Template Actions dialog box opens.

Alternatively, right-click a template monitor or group. The Template actions menu opens.

2 Select **New Alert**. The New Alert window opens.

3 Select the alert type whose definition you want to add to the template. The New Alert window for that alert opens.

4 If you are using template variables, enter the variable syntax for all fields whose values are replaced with a variable. For details, see “Referencing Template Variables” on page 1061.

5. Enter the actual values for any fields that remain constant throughout the template deployment. For details on configuring SiteScope alerts, see “Understanding Alerts” on page 1184.
6. Click **OK** to add the alert configuration to the selected template object.

Tip: You can customize SiteScope alert templates to alter the content and format of alert messages. For details, see “Customizing Alert Templates” on page 1317.

Working with Template Variables

While you can create templates without using template variables, the use of variables is central to the power and utility of templates. Working with SiteScope template variables requires some planning and familiarity with the configuration settings used in SiteScope monitors.

Template variables are substitution markers for monitor configuration settings. You create template variables to represent monitor configuration settings that you want to be able to modify whenever you deploy the template. You reference the variable in a text fields in one or more template monitors. Examples of common uses for template variables are: server or host addresses, disk drive designators, file paths, and monitor name descriptions.

There are two steps you use when working with template variables:

1. Create the template variable in the template. For more information, see “Template Variables” on page 1051 .
2. Reference the variable in one or more configuration objects in the template. For more information, see “Referencing Template Variables” on page 1061.

   Each variable that is referenced in a monitor or group object in a template prompts the display of a corresponding entry field when the template is deployed. The variable name is used as a label for the text entry field.

Some monitor configuration settings can not be set using template variables. With the exception of the remote server selection menu, configuration items that are normally selected using a selection drop-down can not be defined using template variables. Configuration items that are normally selected using a check box or radio selection can not be configured using template variables.

Template variables are always child elements of the template container in which they reside. Variables can be referenced and used to define configuration settings for group, monitor, or alert configuration templates within the template.

You should plan and create the template variables before you create other template objects, such as servers and monitors. This way you can enter the references to the variables into the template monitors, groups, or alerts as you add them to the template. Deleting a template variable that has already been referenced in a template object requires that the referencing object be deleted from the template to clear the broken reference.

Variable Syntax

There are two types of template variables in SiteScope:

- user-defined variables
- system variables

User-defined variables are used to enter text-based values during template deployment. System variables are a set of predefined variables you use to access the list of remote servers known to SiteScope and system time information. Each type of variable has specific syntax conventions which are described in the following sections.

Syntax for User-Defined Variables

User-defined template variables can be alphanumeric characters and may contain the underscore character. They may not contain whitespace, punctuation marks, or other non-alphanumeric characters, except the underscore character. You can create as many variables as you need.

Examples of valid template variable syntax are:

```
description_text
DiskDrive
TARGET_URL
matchExpression
```

You should choose variable names that describe the configuration parameter that is represented. The variable name is used as a label for the variable entry field on the variable value entry window when you deploy the template.

Syntax for System Variables

SiteScope recognizes several pre-defined template variables. These are values that are known by the system, including the list of servers for SiteScope, detected servers such as NetBIOS, as well as user-defined server connection profiles such as remote UNIX. The syntax and description for the pre-defined system variables are:

Syntax for System Variables	Description
SERVER_LIST	Returns a list from which to select one of all the servers known by the platform. Use this to allow selection of remote servers for **Server** or **Host Name** properties only.
SERVER_NAME	This variable is derived from the SERVER_LIST variable. Returns the name of the current server with \\ (backslashes) before the name. Use when referencing the server in other fields.

Syntax for System Variables	Description
SERVER_NAME_BARE	This variable is derived from the SERVER_LIST variable. Returns the name of the current server without \\ (backslashes) before the name. Use when referencing the server in a field requiring just the name of the server (for example when deploying CPU monitors or when referencing the name of the server in a description: “Disk space on server Mail.”
DATE	Returns the system date on the server where SiteScope is running. Use to add the date that a monitor was created to a name or description.
TIME	Returns the system time on the server where SiteScope is running. Use to add the time that a monitor was created to a name or description. The value is the time that the template is actually deployed.

Referencing Template Variables

After you have added template variables to a template, you must create references to them in a monitor or group configuration object. The syntax you use to reference a variable depends on the type of variable.

You reference a user-defined variable using the following syntax in the object's configuration field:

```
%%variable_name%%
```

The reference is both case sensitive and syntax sensitive. The variable_name reference must match the template variable name and be surrounded by double % symbols.

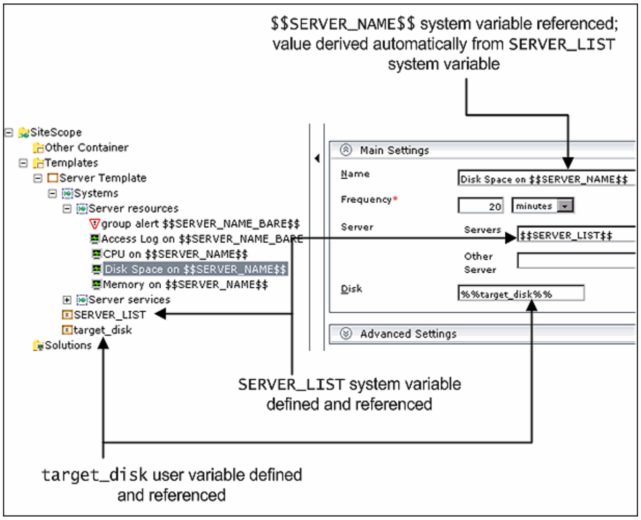
Note: User-defined template variables must be created before they can be referenced in monitor or group configuration templates. Using the %% symbols with a text string that has not already been added to the template as a template variable does not create a reference to a template variable even if a matching variable name is added later.

You reference a system variable using the following syntax in the object's configuration field:

```
$$VARIABLE_NAME$$
```

As with user-defined variables, the reference is both case sensitive and syntax sensitive. The SERVER_LIST variable must be defined explicitly as a variable in the template. As long as this variable is defined, the SERVER_NAME and SERVER_NAME_BARE variables may be used in configuration objects by referencing them using the $$VARIABLE_NAME$$ syntax directly in the monitor or group configuration object. The TIME and DATE variables can also be referenced directly.

The following diagram shows examples of how to reference user-defined variables and the SERVER_LIST and the derived system variables for a monitor template.



Name: Disk Space on $$SERVER_NAME$$
Frequency*: 20 minutes
Server: Servers $$SERVER_LIST$$
Other Server:
Disk: %%target_disk%%

$$SERVER_NAME$$ system variable referenced; value derived automatically from SERVER_LIST system variable

SERVER_LIST system variable defined and referenced

target_disk user variable defined and referenced

Counter Selection in Monitor Templates

SiteScope includes a number of application monitor types that are designed to monitor measurements specific to the target system. These monitor types use a **Get Counters** or **Get Measurements** browser feature in their properties panel. Configuring these monitor types manually requires several steps. After selecting the monitor type, you generally have to specify connection properties to the target system and then request SiteScope to retrieve the measurement counters from the remote system. The next step involves selecting the desired counters to be monitored and adding them to the configuration. After this, the monitor can be added to SiteScope.

Deploying monitors using templates does not accommodate a separate step for counter selection. Another mechanism is used to enable the selection of counters for these monitor types using templates. SiteScope uses text matching or regular expression matching to automate the counter selection step for template deployment. You do use a counter selection step when you create the template monitor.

The simplest method for counter selection in templates is to select the specific counters explicitly in the monitor template. This creates an explicit text match used to select the matching counter during deployment. You use the following steps to add a browsable counter monitor type with explicitly selected counters.

To add a monitor with browsable counters to a template:

1 Right-click the group within the template into which you want to add the monitor configuration. The template group menu opens.

2 Select **New Monitor** from the menu. The New Monitor window opens.

3 Select the monitor type you want to configure for the template. The New Monitor window for that monitor type opens.

4 If you are using template variables, enter the variable syntax for all fields whose values are to be replaced with a variable. This includes use of the SERVER_LIST system variable. For details, see “Referencing Template Variables” on page 1061.

Note: You do not specify an actual server to connect to at this step of the procedure. You are required to enter valid server connection parameters in a following step.

5 Enter the actual values for any fields which remain constant throughout the template deployment. For details on configuring SiteScope monitors, see “Working with SiteScope Monitors” on page 383.

6 Depending on the monitor type, click the **Get Measurements** or **Get Counters** button in the lower portion of the Main Settings section of the Properties tab. The counter selection dialog box opens.

7 Depending on the monitor type, select a server or enter the connection information for a server that is running the service or application that you want to monitor. This may be a duplication of the information you entered for the monitor configuration.

8 When you have selected a valid server or entered the necessary connection information, click the **Get Measurements** or **Get Counters** button in the lower portion of the dialog box to retrieve the available counters. The counter selection dialog box is updated.

9 Select the measurements or counters that you want to monitor. These are the counters configured for each instance of the monitor created when the template is deployed. Use the selection features as applicable to expand or browse the available counters and mark them for selection.

If the specific counters on the target system vary from one deployment to another, you may be able to use a regular expression to match a pattern that represents the type or category of counter you want to monitor. See "Counter Selection Using Regular Expressions" on page 1065 for more information.

10 Depending on the monitor type, click the **Add** button to add the selection to the selection list. Click the **OK** button to confirm the selection. The window closes and the selected counters are displayed in the **Counters** section of the Main Settings panel.

11 Configure the other template monitor properties as applicable.

Note: Once you have selected counters for the template monitor, the counters become available as status threshold parameters in the Threshold Settings section.

12 Click **OK** to add the monitor configuration to the template group.

Counter Selection Using Regular Expressions

Many applications have a number of measurement counters that vary according to the system on which it is running, the configuration of system options, and the components installed. In this case, selecting explicit counters in a monitor template may not be useful across multiple instances of an application or system. Some systems have measurement counters that have a similar pattern but may vary by the name of a node or object context. You can use regular expressions in monitor templates to help automate the selection of multiple measurement counters.

Note: Use of this regular expression counter matching feature requires knowledge of the counters on the system to be monitored. You should manually set up a monitor of the type you want to add to the template and carefully review the counters available on the type of system you want to monitor. Creating a “greedy” regular expression that matches large numbers of counters on a remote system may adversely impact SiteScope performance.

The steps you use to create a template monitor to use regular expressions are very similar to the procedure described in the previous section. Instead of selecting all of the counters to be monitored explicitly, you select one or more counters that are representative of all the counters you want to select. The counter selections in monitor templates are stored as text strings. You edit these strings to create patterns that SiteScope uses to find matching counters that are selected when the monitor is deployed.

Examples

- **Example 1.** The following is a simple example of how a regular expression can be used for counter selection for a SNMP by MIB Monitor type in a template:

  You want to monitor the following three counters from several SNMP agents in your infrastructure:

  ```
  iso/org/dod/internet/mgmt/mib-2/system/sysDescr
  iso/org/dod/internet/mgmt/mib-2/system/sysUpTime
  iso/org/dod/internet/mgmt/mib-2/system/sysName
  ```

  You could select all three counters explicitly in the template monitor. Alternately, you could select one of these and then modify the counter string to be a regular expression such as the following:

  ```
  /iso\/org\/dod\/internet\/mgmt\/mib-2\/system\/sys[DUN][a-zT]*/
  ```

  In this example, the counter selection string has been edited to add a pair of / slashes before and after the string. This is necessary to indicate that the string is to be interpreted as a regular expression. Since the selection string included several / slash characters initially, each of these characters must be escaped by adding a \ backslash character immediately preceding it. The [DUN][a-zT]* string includes two character class declarations commonly used in regular expression syntax. For more information on regular expression syntax, see “Using Regular Expressions” on page 1281.

- **Example 2.** The following is an example of how a regular expression can be used for counter selection for a UNIX Resource Monitor type in a template:

  You want to monitor daemon processes running on several UNIX or Linux servers in your infrastructure. The list of processing running might include the following:

```
Process\-bash\NUMBER RUNNING
Process\../java/bin/java\NUMBER RUNNING
Process\./ns-admin\NUMBER RUNNING
Process\./ns-proxy\NUMBER RUNNING
Process\./ns-sockd\NUMBER RUNNING
Process\/bin/sh\NUMBER RUNNING
Process\/etc/init\NUMBER RUNNING
Process\/usr/apache/bin/httpd\NUMBER RUNNING
Process\/usr/lib/nfs/statd\NUMBER RUNNING
Process\/usr/lib/saf/sac\NUMBER RUNNING
Process\/usr/lib/saf/ttymon\NUMBER RUNNING
Process\/usr/lib/snmp/snmpdx\NUMBERRUNNING
Process\/usr/lib/ssh/sshd\NUMBER RUNNING
...
```

  You can create a regular expression counter selection string to match only those processes that end with the letter “d”. The following is an example regular expression to match this pattern:

```
/Process[\W\w]{5,18}d[\W]{1,2}NUMBER RUNNING/
```

  As with Example 1, the counter selection string includes / slashes before and after the string to indicate that the string is a regular expression. The example process strings on the UNIX server include combinations of \ back slash and / forward slash characters. Since these characters have special meaning in regular expressions, they would have to be escaped. This can be complicated since the process strings have many variations and combinations of these and other symbols. The example regular expression used here simplifies the expression by using character class declarations. The [\W] class is used to match punctuation marks. This matches on the \, -, :, and / characters that appear in some of the process strings without the need to escape the characters individually. For more information on regular expression syntax, see “Using Regular Expressions” on page 1281.

Modifying Counter Selection Strings to Use Regular Expressions

You can modify counter selection strings for template monitors to use regular expressions when you create the monitor or you can edit the monitor later. You use the following steps to modify a template monitor to use a regular expression for measurement counter selection.

To modify a template monitor for regular expression counter matching:

1. If necessary, right-click the monitor template you want modify. The template monitor menu opens. Click **Edit** to open the template monitor properties view.

   In the Main Settings panel, select a counter selection string that is representative of the pattern of counters you want to configure for the monitor. In the **Selected Measurements** or **Counter Name** section (depending on the monitor type), click the Edit button to the right of the counter string you want to edit. A string edit dialog opens.

2. Modify the counter selection string to be a regular expression by adding a slash (“/”)character to the beginning and end of the string. Modify the string to use other pattern matching syntax as appropriate. For more information on regular expression syntax, see “Using Regular Expressions” on page 1281.

3. Click the **OK** button at the bottom of the edit dialog box. The dialog box closes and the counter selection string is updated in the Main Settings panel.

   If the template monitor was configured with explicit counter selections that can be matched using the regular expression that was entered, you can delete the extra counter strings by clicking the Delete button to the right of the counter string.

4. Click the **OK** button at the bottom of the monitor Properties tab to update the template monitor configuration.

Using Templates to Deploy SiteScope Monitoring

You deploy SiteScope monitoring using templates by a copy and paste operation within the monitor tree. The paste operation opens a template value dialog where you specify values for any template variables used in your template objects. You use the following steps to deploy templates.

To deploy a SiteScope monitor configuration template:

1. Expand the applicable template container in the monitor tree and select the template folder you want to deploy. Right-click the template. The templates action menu opens.
2. Choose **Copy**.
3. In the monitor tree, right-click the SiteScope node or SiteScope group container where you want to deploy the template. The container's menu opens.
4. Choose **Paste**. The Variable Values input window opens in the content area. The entry fields displayed correspond to the template variables used in the template objects. For example, if there is a template variable named server_id which is used in a Disk Space and a Memory monitor defined in the template, an entry field labeled **server_id** is displayed in the Variable Values input window. The value you select or enter is used for each monitor that references the server_id variable.
5. Enter the required variable values in the entry fields displayed.

   If you used the SERVER_LIST pre-defined variable definition, the entry field is a list of available remote server values detected by the system. The system variables SERVER_NAME and SERVER_NAME_BARE return values based on the server selected in the **SERVER_LIST** item.
6. Click **OK** to finish the deployment.

   SiteScope makes the variable value substitutions and adds the applicable elements to the monitor tree.

Exporting and Importing Templates

Templates can be exported for use on other SiteScope installations. This allows you to efficiently replicate standardized monitor configurations across the enterprise.

Note: SiteScope templates are stored as binary data. This is different from the text-based monitor sets used in earlier versions of SiteScope. Any changes to templates must be performed using the SiteScope interface.

You export and import templates by using a template container's right-click menu. One or more templates can be exported to a single file. You use the following steps to export templates from SiteScope.

To export templates from SiteScope:

1. Click the template container object in the monitor tree that contains the template or templates you want to export. The Export Template window opens.
2. Enter a valid file name in the **Export File Name** field. Use a name that is descriptive of the template or templates to be exported.
3. The default location for exported templates is the <SiteScope_install_path>\SiteScope\export. To have the file saved to a different location, enter the location in the **File Path** field.
4. Use the Templates to Export menu tree to select the templates you want to export. By default, all templates within the template container are exported. Use the check boxes to the left of the template names to select or deselect templates.
5. Click the **OK** button to export the templates. SiteScope creates an export file using the information you entered.

Once you have exported templates, you can copy the export file to another SiteScope server and import the template configuration. Make a note of the exact filename and location where you copy the file. You use the following steps to import a template.

To import templates into SiteScope:

1. Click the template container object in the monitor tree into which you want to import the template or templates. The Import Template window opens.
2. Enter the name of the file you want to import in the **Import File Name** field.
3. Enter the path to file to be imported in the **File Path** field. The default location for importing templates is <SiteScope_install_path>\SiteScope\export.
4. Click the **OK** button to import the templates. Templates contained in the file are added to the template container. The imported templates can be used directly or modified as needed.

54

SiteScope Solution Templates Overview

The range of monitor types available with SiteScope gives you flexibility in monitoring a variety of systems and services. With the increasing complexity of current network applications, it is difficult to know the most effective way to monitor key systems and services. SiteScope solution templates are designed to provide rapid deployment of performance and availability monitoring optimized for specific applications and services.

About Solution Templates

Solution templates are special monitor set templates designed to monitor popular enterprise applications and network systems. You use solution templates to deploy a combination of standard SiteScope monitor types and solution-specific monitors with settings that are optimized for monitoring the availability, performance, and health of the target application or system. For example, the solutions for Microsoft Exchange monitoring include performance counter, event log, and Exchange application specific monitor types.

The following table lists solution templates available for SiteScope. The following sections contain more information about each solution and the solution specific monitor types:

Solution Name	Description
Active Directory Solution Template	Monitors the performance and efficiency of Microsoft domain controllers.
AIX Host Solution Templates	Monitors performance, availability, and health for AIX host machines.
Exchange Solution Templates	Includes individual solution options for monitoring application health, message flow, and usage statistics for Exchange Server 5.5, Exchange Server 2000, or Exchange Server 2003.
Linux Host Solution Templates	Monitors performance, availability, and health for Linux host machines.
Oracle Solution Template	Monitors performance, availability, and usage statistics for Oracle 8i, 9i, and 10g databases.
SAP Solution Templates	Monitors performance, availability, and usage statistics for SAP system components.
Siebel Solution Templates	Monitors performance, availability, and usage statistics for Siebel Application Server installed on Microsoft Windows and UNIX operating systems.
Solaris Host Solution Templates	Monitors performance, availability, and health for Solaris host machines.

WebLogic Solution Template	Monitors performance, availability, and usage statistics for BEA WebLogic application servers.
WebSphere Solution Template	Monitors performance, availability, and usage statistics for IBM WebSphere Server 5.x application servers.
Windows Host Solution Template	Monitors performance, availability, and health for Windows 2000, Windows XP, and Windows Server 2003 host machines.

Working with Solution Templates

The following is an overview of the steps for deploying solution templates:

1. Request the applicable Solution license from Customer Support.
2. Enter the license into the SiteScope product using the General Preferences page.
3. Open or create a monitor group into which you want to deploy the solution monitors.
4. Select the applicable solution template.
5. Copy and paste the solution template to the target monitor group container.
6. Complete the Solution Template Variable Values page as indicated.
7. Configure alerts and reports for newly created solution monitors.

Troubleshooting Solution Templates

There are times when, if SiteScope is not running properly, it is advised to delete the contents of SiteScope's persistency directory located in <**SiteScope root directory**>/**persistency**. The installed solution sets are located in this directory and if its contents are deleted, the solution sets no longer appear in the monitor tree and cannot be used. To reactivate the solution sets, you must copy the install files back into the persistency directory.

To reactivate the solution template files:

1. Locate the solution template files in the following directory: <**SiteScope root directory**>/**export**.
2. Copy the contents of <**SiteScope root directory**>/**export** into <**SiteScope root directory**>/**persistency/import**.
3. Check that the solution templates have been reinstalled by locating them in the monitor tree.

55

Active Directory Solution Template

To address the needs of Active Directory performance monitoring, HP offers the Active Directory Solution. The SiteScope Active Directory Solution provides monitoring of domain controller performance, services on which Active Directory depends, and distributed Active Directory performance.

Understanding the Active Directory Solution

The Active Directory Solution Template deploys a set of monitors against a particular Domain Controller. These monitors encompass best practices monitoring for Active Directory. This template includes NT Event Log, Service, LDAP, performance counter and Active Directory Replication monitors.

Note: You must have the applicable SiteScope option license to use the Active Directory solution templates. Contact your HP sales representative for more information about Solution licensing.

The purpose of a solution template is to provide comprehensive monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the Active Directory Solution Template include:

- Reduces the need for Active Directory performance domain expertise
- Reduces the time to configure and deploy Active Directory monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds no overhead to production systems

The Active Directory Solution Template deploys monitors that target the following aspects of Active Directory performance:

- **Domain controller performance.** This category refers to the low level health of each domain controller in the environment. The Active Directory Solution Template automatically configures monitors for domain controller health.
- **Dependent services.** Active Directory depends on several key services. Without these services, Active Directory can become unresponsive or fail altogether. The Active Directory Solution Template automatically configures monitors for a list of important services upon which Active Directory performance is dependent.
- **Distributed Active Directory performance.** Perhaps the most important aspect and key indicator of Active Directory performance is how fast Active Directory is replicating changes out to all domain controllers. The Active Directory Solution Template automatically configures monitors for monitoring and testing replication of changes and updates.

An in depth description of the Active Directory Solution is available in the SiteScope Active Directory Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_Active_Directory_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Active Directory Solution license key from HP.

After the solution template is deployed the monitors created behave the same as other monitors in SiteScope. This means that they can be viewed, edited, and deleted like other monitors.

Note: Some of the monitor types deployed by the solution templates can only be added to SiteScope by using the Active Directory Solution sets. For more information, see the section for the particular monitor types.

Deploying the Active Directory Solution Template

Deploy one Active Directory Solution Template for each domain server in your environment. Use the following steps to deploy an Active Directory Solution Template.

To deploy an Active Directory Solution Template:

1. Click on the SiteScope container into which you want to add the Active Directory Solution and expand the container to display the group containers.
2. Right-click the Active Directory Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the Active Directory Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the Active Directory Solution Variable Values form as described in the section Active Directory Solution Template Settings below. When the required items are completed, click the **OK** button.

6 As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

Deploying the Active Directory Solution creates a new monitor group container in which the individual solution monitors are added.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution templates do not configure any automated alerts for the monitors created. You may create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Active Directory Solution Template Settings

Server_List

Choose the Domain Controller that you want to monitor. Click the **choose server** link to monitor services or processes on another server (may require that you define connections to other servers).

Host_Name

Type in the host part of the domain controller's hostname (do not include the fully qualified domain name).

Replicating_Domain_Controllers

Type in a comma separated list of domain controllers that replicate data from the domain controller selected above.

LDAP_Security_Principal

Enter in LDAP Security Principal of a Domain Admin account. For Active Directory this is in the format of cn=Domain Admin User,cn=users,dc=yoursite,dc=com.

Password

Enter in the password for the user selected above.

Logical_Drive

Enter in the logical drive that this Domain Controller is using for its database and log files.

Global Catalog (AD with Global Catalog ONLY)

If the Domain Controller is a Global Catalog server then select this box.

Active Directory Solution Metrics

Categories and metrics available for monitoring with the Active Directory Solution include:

Active Directory Application

- LSASS\Private Bytes
- NTDS\DRA Inbound Bytes Compressed (Between Sites, After Compression)/sec.
- NTDS\DRA Outbound Bytes Compressed (Between Sites, After Compression)/sec.
- NTDS\DRA Outbound Bytes Not Compressed (Within Site Since Boot)/sec.
- NTDS\DRA Outbound Bytes Total/sec.
- NTDS\DS Search Sub-operations/sec.
- NTDS\KDC AS Requests/sec.
- NTDS\KDC TGS Requests
- NTDS\LDAP Client Sessions
- NTDS\LDAP Searches/sec.

- NTDS\NTLM Authentications/sec.
- Process\Handle Count - LSASS

Service Checks

- FRS (File Replication Service)
- Intersite Messaging
- Kerberos Key Distribution Center
- Netlogon
- Sysvol
- Windows Time

Core Operating System

- Memory\Available MBytes
- Memory\Page Faults/sec.
- Physical Disk\Current Disk Queue Length
- Processor % DPC Time_Total (instance)
- Processor\% Processor Time -_Total
- System\Context Switches/ sec.
- System\Processor Queue Length
- System\System Up Time

56

AIX Host Solution Templates

The AIX Host Solution Template allows you to monitor any host which runs a supported version of an AIX operating system. This solution gathers generic metrics that represent the health, availability and performance of the target AIX machine.

Understanding the AIX Host Solution

This solution is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the AIX host. The template supports the versions of AIX that are supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can generate a Server Centric Report which displays data from three different metrics about the server being monitored. It is recommended to use Solution Templates when creating the UNIX Resource Monitor, since the appropriate monitors and metrics are already configured. For more information on generating a Server Centric Report, see “Generating a Server Centric Report” on page 337.

Note: You must have the applicable SiteScope option license to use the AIX Host Solution Template. Contact your HP sales representative for more information about Solution licensing.

The AIX Host Solution Template provide comprehensive AIX operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the AIX Host Solution Template include:

- Reduces the need for AIX performance domain expertise
- Reduces the time to configure and deploy various performance monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds only negligible overhead to production systems

The AIX Host Solution Template deploys monitors that target the following aspects of AIX performance and health:

- CPU status and utilization details
- Memory status and utilization details
- File system status and utilization details

An in depth description of the AIX Host Solutions settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_OS_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

System Requirements

The AIX Host Solution license must be applied to the SiteScope server onto which you want to deploy the AIX Host Solution. See “SiteScope General Preferences” on page 226 for details on how to enter license information.

Before you can use the AIX Host Solution Template, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the target AIX host.
- The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test. For details, See “UNIX Remote Preferences Overview” on page 201.
- The SiteScope server itself can also be monitoring if it runs a supported AIX operating system.
- The template supports the AIX versions supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

Deploying the AIX Solution Template

Deploy one AIX Solution Template for each AIX server in your environment. Use the following steps to deploy an AIX Host Solution Template.

To deploy an AIX Host Solution Template:

1. Click the SiteScope container into which you want to add the AIX Host Solution and expand the container to display the group containers.
2. In the left tree, expand **Solution Templates**.
3. Right-click the **AIX Host** solution template to display the action menu and select **Copy**.
4. Select the SiteScope container or the monitor group container into which you want to deploy the solution template.
5. Right-click the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.

6 In the **SERVER_LIST** list-box, select the AIX remote for which you want to deploy the solution. You can also deploy on the SiteScope server by selecting **SiteScope Server** in the list-box. Click the **OK** button.

7 If some of the monitors failed to deploy, a paste results message is shown listing the names of the monitors created along with messages describing the error. After viewing the message, select **Close**.

Deploying the AIX Host Solution Template creates a new monitor group container in which the individual solution monitors are added. The monitor group container is assigned a name in the format AIX monitors for <server_name> where server_name is the server selected from the **Server_List** field.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution Templates do not configure any automated alerts or reports for the monitors created. You may create and associate one or more alert definitions or reports to the monitors or monitor groups created by solution templates.
- The AIX Host Solution Template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Service Centric Report support.

57

Exchange Solution Templates

To address the needs of Microsoft Exchange performance monitoring, HP offers Exchange solutions. The SiteScope Exchange Solution Templates provide monitoring of performance, availability, and usage statistics for Microsoft Exchange 5.5, 2000, and 2003 servers.

Understanding the SiteScope Exchange Solution

The SiteScope Exchange Solution includes three solution templates that implement best practice monitoring for Microsoft Exchange messaging services. This includes solution templates for the following:

- Exchange 5.5
- Exchange 2000
- Exchange 2003

You use these solution templates to deploy a set of monitors that test the health, availability, and performance of an Exchange server. Depending on the set chosen, this set includes monitors checking NT Event log entries, MAPI operations, system performance counters, and message system usage statistics.

Note: You must have the applicable SiteScope option license to use the Exchange Solution templates. Contact your HP sales representative for more information about Solution licensing.

The Exchange Solution templates provide comprehensive Exchange system monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the Exchange Solution templates include:

- Reduces the need for Exchange performance domain expertise
- Reduces the time to configure and deploy Exchange monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds no overhead to production systems

The Exchange solution templates deploy monitors that target the following aspects of Exchange performance and health:

- **Basic server/OS performance.** This category refers to the system-level health of a server. The Exchange Solution Template automatically configures monitors for server health.
- **Application performance.** Application performance is a measure of how well specific Exchange components are functioning. The Exchange Solution Template automatically configures monitors for a list of important Exchange application components.
- **Mail protocol response time.** Perhaps the most important aspect and key indicator of Exchange performance is mail protocol response time. While Exchange can utilize many protocols, the MAPI protocol is commonly used in Microsoft networks.

- **Usage statistics.** The last category related to Exchange performance is usage. While usage in and of itself is not necessarily a key indicator of performance, changes in usage can affect overall Exchange performance. In addition, Exchange usage statistics help IT organizations spot trends and plan for the future. The Exchange Solution Template automatically configures monitors for a list of important Exchange usage parameters.

An in depth description of the Exchange Solution is available in the SiteScope Exchange Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_Exchange_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Exchange Solution license key from HP.

After the solution template is deployed the monitors that are created behave the same as other monitors in SiteScope. This means that they can be viewed, edited, and deleted like other monitors.

Note: Some of the monitor types deployed by the solution templates can only be added to SiteScope by using the Exchange Solution templates. See the section for the particular monitor types for more information.

System Requirements

The Exchange Solution license must be applied to the SiteScope server onto which you want to deploy the Exchange Solution. See the section on SiteScope General Preferences for details on how to enter license information.

Important: Each of the Exchange solutions make use of the SiteScope MAPI Monitor. Successful deployment of this monitor type requires specific setup configuration relating to the mailbox owners and the SiteScope service. For the MAPI Monitor system requirements, see “MAPI Monitor Overview” on page 508. This details the steps you need to perform before deploying an Exchange Solution Template.

Deploying Exchange Solution Templates

Deploy one Exchange Solution Template for each Exchange server in your environment. Use the following steps to deploy an Exchange Solution Template.

To deploy an Exchange Solution Template:

1. Click on the SiteScope container into which you want to add the Exchange Solution and expand the container to display the group containers.
2. Select the Exchange Solution template that matches the version of Microsoft Exchange that you want to monitor.
3. Right-click the solution template icon to display the action menu and select **Copy**.
4. Select the SiteScope container or the monitor group container into which you want to deploy the Exchange Solution.
5. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.

6 Complete the items on the Exchange Solution Variable Values form as described in the section "Exchange Solution Template Settings" below. When the required items are completed, click the **OK** button.

7 As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

Deploying the Exchange Solution creates a new monitor group container in which the individual solution monitors are added. The monitor group container is assigned a name of the format Exchange *version_number* on *server_name* where *server_name* is the server selected from the **Server_List** field.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution Templates do not configure any automated alerts for the monitors created. You may create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Exchange Solution Template Settings

Server_List

Choose the server on which the Exchange server that you want to monitor is running from the selection list. If the server you want to monitor is not in the list, you need to define a connection profile to the server. See the section on "Windows Remote Preferences Overview" on page 195 for the steps you use to create a Windows connection profile.

Mail_User

Enter the Windows account login name for the user for which e-mail round trip times are tested using MAPI.

Mail_Password

Enter the Windows account login password for the user name entered above.

Mailbox

Enter the name (alias) of the mailbox to be used for testing e-mail round trip times using MAPI. This is often the e-mail account name but it may be a different name. It is recommended that you copy the mailbox name as it appears in the E-Mail Account properties for the e-mail account you are using for this solution.

Mail_Domain

Enter the domain to which both the owner of the mailbox being used and the Microsoft Exchange server belong.

Note: The owner of the mailbox to be used by this solution must also have administrative account privileges on the machine where SiteScope is running. SiteScope also needs user account access to the domain where the Microsoft Exchange server is running.

WMI_User (Exchange 2003 ONLY)

Enter the user name to use when querying the server for mailbox and public folder statistics. The statistics are gathered via WMI (Windows Management Instrumentation), so the user name entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2. If this field is left blank, the user that SiteScope is running as is used.

WMI_Password (Exchange 2003 ONLY)

Enter the password for the user entered above for gathering WMI statistics, or leave this blank if user field is left blank.

Exchange Solution Metrics

Metrics available for monitoring with Exchange Solution for Microsoft Exchange include:

Exchange Application (Exchange 5.5)

The metrics below apply to MTA instances:

- MSExchangeDS:AB Browses/sec
- MSExchangeDS:AB Reads/sec
- MSExchangeIMC: Connections Inbound
- MSExchangeIMC: Connections Outbound
- MSExchangeIMC: Messages Entering MTS-IN
- MSExchangeIMC: Messages Entering MTS-OUT
- MSExchangeIMC: Messages Leaving MTS-IN
- MSExchangeIMC: Messages Leaving MTS-OUT
- MSExchangeIMC:Queued Inbound
- MSExchangeIMC:Queued MTS-IN
- MSExchangeIMC:Queued MTS-OUT
- MSExchangeIMC:Queued Outbound
- MSExchangeIS Private:Message Recip. Deliv./min

- MSExchangeIS Private:Messages Submitted/min
- MSExchangeIS Private:Receive Queue
- MSExchangeIS Private:Send Queue
- MSExchangeIS Private:Single Instance Storage Ratio
- MSExchangeIS Public:Message Recip. Deliv./min
- MSExchangeIS Public:Message Submitted/min
- MSExchangeIS Public:Receive Queue
- MSExchangeIS Public:Send Queue
- MSExchangeIS:AB RPC Packets/sec
- MSExchangeIS:Active Anonymous Connection Count
- MSExchangeIS:Active Connection Count
- MSExchangeIS:Active User Count
- MSExchangeMTA:Adjacent MTA Associations
- MSExchangeMTA:Work Queue Length
- MTA Connection Instances
- MTA Connections:Last Outbound Association
- MTA Connections:Next Association Retry
- MTA Connections:Oldest Message Queued
- MTA Connections:Queue Length

Exchange Database (Exchange 5.5)

- Database:File Bytes Read/sec:All Instances
- Database:File Operations Pending:Directory
- Database:File Operations Pending:Information Store
- Database:Log Record Stalls/sec
- Database:Log Threads Waiting:All Instances

Core Operating System (Exchange 5.5)

- % Free Space
- Memory\Available Mbytes
- Memory\page reads/sec
- Memory\page writes/sec
- Memory\pages/sec
- Network Interface(netcard)Bytes Total/sec
- PhysicalDisk (_Total) Current Disk Queue Length
- PhysicalDisk (_Total) Avg. Disk Queue Length
- PhysicalDisk (_Total) Avg. Disk sec/Read
- PhysicalDisk (_Total) Avg. Disk sec/Write
- Process (dsamain): % processor time
- Process (emsmta): % processor time
- Process (mad): % processor time
- Process (store): % processor time

Exchange Application (Exchange 2000/2003)

Examples of metrics available for monitoring with Exchange Solution for Microsoft Exchange 2000 and Microsoft Exchange 2003 include:

- Epoxy(protocol)\Client Out Que Len
- Epoxy(protocol)\Store Out Que Len
- MSExchange IS Mailbox\Message Opens/sec
- MSExchangeDSAccess Caches\Cache Hits/sec
- MSExchangeDSAccess Caches\Cache Misses/sec
- MSExchangeDSAccess Caches\LDAP Searches/sec
- MSExchangeIS Mailbox\Folder Opens/sec
- MSExchangeIS Mailbox\Local Delivery Rate
- MSExchangeIS\RPC Operations/sec
- MSExchangeIS\RPC Requests
- MSExchangeIS\VM Largest Block Size
- MSExchangeMTA\Messages/sec
- SMTP Server\Local Queue Length
- SMTP Server\Messages Delivered/sec
- SMTP Server\Messages Received/sec
- SMTP Server\Messages Sent/sec

Exchange Database (Exchange 2000/2003)

- Database Cache Size
- Log Record Stalls/sec
- Log Writes/sec

Core Operating System (Exchange 2000/2003)

- % Free Space
- Memory\Available MBytes
- Memory\page reads/sec
- Memory\page writes/sec
- Memory\pages/sec
- Network Interface(netcard)Bytes Total/sec
- PhysicalDisk (_Total) Average Disk Queue Length
- PhysicalDisk (_Total) Avg. Disk sec/Read
- PhysicalDisk (_Total) Avg. Disk sec/Write
- PhysicalDisk (_Total) Current Disk Queue Length
- Process (inetinfo)\% Processor Time
- Process (inetinfo)\Working set
- Process (system)\% Processor Time
- Process (system)\Working set
- Processor (_Total)\% Processor Time

58

Linux Host Solution Templates

The Linux Host Solution Template allows you to monitor any host which runs a supported version of a Linux operating system. This solution gathers generic metrics that represent the health, availability and performance of the target Linux machine.

Understanding the Linux Host Solution

This solution is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the Linux host. The template supports the versions of Linux that are supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can generate a Server Centric Report which displays data from three different metrics about the server being monitored. It is recommended to use Solution Templates when creating the UNIX Resource Monitor, since the appropriate monitors and metrics are already configured. For more information on generating a Server Centric Report, see “Generating a Server Centric Report” on page 337.

Note: You must have the applicable SiteScope option license to use the Linux Host Solution Template. Contact your HP sales representative for more information about Solution licensing.

The Linux Host Solution Template provide comprehensive Linux operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the Linux Host Solution Template include:

- Reduces the need for Linux performance domain expertise
- Reduces the time to configure and deploy various performance monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds only negligible overhead to production systems

The Linux Host Solution Template deploys monitors that target the following aspects of Linux performance and health:

- CPU status and utilization details
- Memory status and utilization details
- File system status and utilization details

An in depth description of the Linux Host Solutions settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_OS_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

System Requirements

The Linux Host Solution license must be applied to the SiteScope server onto which you want to deploy the Linux Host Solution. See "SiteScope General Preferences" on page 226 for details on how to enter license information.

Before you can use the Linux Host Solution Template, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the target Linux host.
- The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test. For details, See "UNIX Remote Preferences Overview" on page 201.
- The SiteScope server itself can also be monitoring if it runs a supported Linux operating system.
- The template supports the Linux versions supported by SiteScope. For details, see "System Requirements" in the *HP SiteScope Deployment Guide* PDF.

Deploying the Linux Solution Template

Deploy one Linux Host Solution Template for each Linux server in your environment. Use the following steps to deploy a Linux Host Solution Template.

To deploy a Linux Host Solution Template:

1. Click the SiteScope container into which you want to add the Linux Host Solution and expand the container to display the group containers.
2. In the left tree, expand **Solution Templates**.
3. Right-click the **Linux Host** solution template to display the action menu and select **Copy**.
4. Select the SiteScope container or the monitor group container into which you want to deploy the solution template.
5. Right-click the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.

6 In the **SERVER_LIST** list-box, select the Linux remote for which you want to deploy the solution. You can also deploy on the SiteScope server by selecting **SiteScope Server** in the list-box. Click the **OK** button.

7 If some of the monitors failed to deploy, a paste results message is shown listing the names of the monitors created along with messages describing the error. After viewing the message, select **Close**.

Deploying the Linux Host Solution Template creates a new monitor group container in which the individual solution monitors are added. The monitor group container is assigned a name in the format Linux monitors for <server_name> where server_name is the server selected from the **Server_List** field.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution Templates do not configure any automated alerts or reports for the monitors created. You may create and associate one or more alert definitions or reports to the monitors or monitor groups created by solution templates.
- The Linux Host Solution Template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Service Centric Report support.

59

.NET Solution Templates

The .NET Solution Template allows you to monitor .NET applications of servers that run a Windows operating system. This solution template deploys a set of monitors that test the health, availability, and performance of an application on the Windows host.

Understanding the .NET Solutions

This solution uses templates you can use to deploy a collection of Windows Monitors configured with default metrics that test the health, availability, and performance of a .NET application and .NET environment. The template supports Windows 2000, Windows XP, and Windows Server 2003.

Note: You must have the applicable SiteScope option license to use the .NET Solution templates. Contact your HP sales representative for more information about Solution licensing.

The .NET Solution templates provide comprehensive .NET monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the .NET Solution templates include:

- Reduces the need for .NET performance domain expertise
- Reduces the time to configure and deploy .NET monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds no overhead to production systems

The .NET solution templates deploy monitors that target the following aspects of .NET performance and health:

.NET CLR Data

This category refers to the common language runtime data (environment of .NET applications). It is designed to check several resource statistics for the .NET CLR for selected application. The .NET Solution Template automatically configures monitors for server health.

ASP.NET

This category is designed to check several resource statistics for the ASP.NET. It gathers common information about application restarts and whole ASP.NET system stability. The .NET Solution Template automatically configures monitors for server health.

ASP.NET Applications

This category is designed to check several resource statistics for the selected ASP.NET application. It gathers common information about application cache, errors, and other critical information. The .NET Solution Template automatically configures monitors for server health.

After the solution template is deployed the monitors that are created behave the same as other monitors in SiteScope. This means that they can be viewed, edited, and deleted like other monitors.

An in depth description of the .NET Solution is available in the SiteScope .NET Best Practices document. This document can be found at <**SiteScope root directory**>**\sisdocs\pdfs\SiteScope_NET_Best_Practices.pdf**. This is a password protected document. The password is provided along with the .NET Solution license key from HP.

System Requirements

The .NET Solution license must be applied to the SiteScope server onto which you want to deploy the .NET Solution. See "SiteScope General Preferences" on page 226 for details on how to enter license information.

Before you can use the .NET Solution, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the target Windows host. Use the Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Windows Resource monitor may require special configuration. For details, see "Windows Resources Monitor Overview" on page 544.
- The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test. Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, See "Configure SiteScope to Monitor a Remote Windows Server" on page 218.
- The SiteScope server itself can also be monitoring if it runs a supported Windows operating system.
- The template supports Windows 2000, Windows XP, and Windows Server 2003.

Deploying .NET Solution Templates

Deploy one .NET Solution Template for each Windows server in your environment. Use the following steps to deploy a .NET Solution Template.

To deploy a .NET Solution Template:

1 Click the SiteScope container into which you want to add the .NET Solution and expand the container to display the group containers.

2 In the left tree, expand **Solution Templates**.

3 Right-click the .NET solution template (**.NET CLR Data**, **ASP.NET**, or **ASP.NET Applications**) to display the action menu and select **Copy**.

4 Select the SiteScope container or the monitor group container into which you want to deploy the .NET Solution.

5 Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.

6 In the **Server** box, enter the address of the Windows remote for which you want to deploy the solution. You can also deploy on the SiteScope Server by entering SiteScope Server in the box.

For ASP.NET Applications template only, in the **ASP.NET Application** box, enter the name of the ASP.NET application you want to monitor. The name must be as it appears in the Task Manager.

For .NET CLR Data template only, in the **Instance** box, enter the name of the application you want to monitor. The name must be the same as it appears in the Task Manager, or can be whole system statistics (by default).

Click the **OK** button.

7 If some of the monitors failed to deploy, a paste results message is shown listing the names of the monitors created along with messages describing the error. After viewing the message, select **Close**.

8 Repeat for each server and for each .NET Solution template required.

Deploying the .NET Solution creates a new monitor group container in which the individual solution monitors are added. The monitor group container is assigned a name in the format <.NET Solution Template> on <server_name> where server_name is the server selected from the **Server_List** field.

Note:

➤ Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.

➤ Solution Templates do not configure any automated alerts or reports for the monitors created. You may create and associate one or more alert definitions or reports to the monitors or monitor groups created by solution templates.

60

Oracle Solution Template

To address the needs of Oracle database performance monitoring, HP offers the Oracle Database Solution. The SiteScope Oracle Database Solution provides efficient and thorough monitoring of performance, availability, and usage statistics for Oracle 8i, 9i and 10g databases.

Understanding the Oracle Database Solution

This solution uses a new monitor type called the Database Counter Monitor. This monitor collects performance metrics from JDBC-accessible databases. In addition to the new monitor type, you can use the Oracle Database Solution Template to deploy a collection of monitors configured with default metrics.

Note: You must have the applicable SiteScope option license to use the Oracle Database Solution Template. Contact your HP Sales representative for more information about Solution licensing.

The purpose of a solution template is to provide comprehensive Oracle database monitoring without requiring the SiteScope user or the IT organization to be an expert on the application.

An in depth description of the Oracle Database Solution is available in the SiteScope Oracle Database Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_Oracle_Database_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Oracle Database Solution license key from HP.

Benefits of the Oracle Database Solution Template include:

- Reduces the need for Oracle performance domain expertise
- Reduces the time to configure and deploy Database Counter Monitors against Oracle databases
- Helps identify both real-time performance bottlenecks and longer term trends
- Ensures that SiteScope monitoring license points are not wasted on lower priority monitors and metrics

The Oracle Database Solution Template deploys monitors that target the following aspects of Oracle performance and health:

General System Statistics

The most important V$SYSSTAT statistics are monitored by default in the monitors deployed by the Oracle Database Solution. Where applicable, these metrics are combined to calculate deltas and rates on a per-second or per-transaction basis. When monitoring the important metrics from the V$ tables in the database, the Oracle Database Solution is a replacement for manually generated SQL scripts.

Oracle Logs

Important Oracle log files are monitored for ORA- errors. Users may customize these monitors to look for specific text in a log file, depending on their database configuration.

Diagnosing Database Problems

In addition to the deployed monitors, Oracle Solution offers several tools that can be used to gain diagnostic information about a database. Resource-intensive SQL statements, shared server process contention, and the number of sessions waiting for specific events are all examples of the diagnostic data that these tools can provide.

Deploying Oracle Database Solution Templates

The SiteScope Oracle Database Solution Template facilitates the implementation of best-practice monitoring of Oracle databases with a minimum of configuration. This solution can be used with Oracle 8i, 9i, and 10g databases.

You use this solution template to deploy a set of monitors that test the health, availability, and performance of an Oracle database. The deployed monitors check general system statistics, such as cache hit ratios and disk I/O, and include tools that provide diagnostic information about important aspects of the database.

This section includes the following topics:

- “Usage Guidelines” on page 1112
- “Oracle Database Solution Template Main Settings” on page 1114
- “Oracle Database Solution Metrics” on page 1115

Usage Guidelines

Use the Oracle Database Solution to monitor statistics from Oracle 8i, 9i, 10g databases. Important system metrics are computed with data retrieved from system tables in the Oracle database. A wide range of Oracle system tables such as V$SYSSTAT, V$LATCH, V$ROLL_STAT, and V$BUFFER_POOL_STATISTICS are consulted to produce these metrics. In this way, the Oracle Database Solution implements the equivalent of many of the system monitoring scripts that come bundled with the Oracle installation.

Before configuring the Oracle Database Solution for deployment, consult the documentation for the Database Counter Monitor (see "Database Counter Monitor Overview" on page 466) and the Log File Monitor (see "Log File Monitor Settings" on page 737) for information about some of the prerequisites and parameters required by the solution template. For example, you find more information on installing the Oracle JDBC driver needed to communicate with the database and the format of the log file path name parameter.

To deploy an Oracle Database Solution Template:

1. Click on the SiteScope container into which you want to add the Oracle Database Solution and expand the container to display the group containers.
2. Right-click the Oracle Database Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the Oracle Database Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Oracle Database Solution Variable Values form opens in the contents panel.
5. Complete the items on the Oracle Database Solution Variable Values form as described in the section "Oracle Database Solution Template Main Settings" on page 1114. When the required items are completed, click the **OK** button.

6 As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- If the monitor was successfully created but the monitor is disabled, you must configure its counters and then manually enable the monitor.
- Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Oracle Database Solution Template Main Settings

Name

The name of the monitor.

Frequency

The frequency in seconds at which you'd like the deployed monitors to run. It is generally a good idea to enter a conservative frequency (10 minutes or greater) when first deploying the solution because some of the SQL queries invoked by the deployed monitors could impose some overhead on the database. Once the monitors are deployed, you can edit the monitors individually and increase the frequencies on specific monitors, if necessary.

Database Connection URL

Enter the connection URL to the database you want to connect to. The syntax is jdbc:oracle:thin:@<server name or ip address>:<database server port>:<sid>.

For example, to connect to the ORCL database on a machine using port 1521 you would use:

jdbc:oracle:thin:@206.168.191.19:1521:ORCL.

Note: The colon and @ symbols must be included as shown.

Database Driver

The name of the JDBC driver to be used by this monitor. Each driver supports a specific connection URL pattern, so it must match the URL entered in **Database Connection URL**.

Database User Name

Enter the user name that SiteScope should use to connect to the database.

Database Password

Enter the password for the user name that SiteScope should use to connect to the database.

Server

Choose the server you want to monitor. Click the choose server link to open the server selection page. Select a server from the drop-down menu or enter an UNC path for the server you want to monitor.

Oracle Alert Log Path

Enter the full path to the Oracle alert log. Consult your database administrator or the Oracle documentation for information on how to access this file.

Oracle Listener Log Path

Enter the full path to the Oracle listener log. Consult your database administrator or the Oracle documentation for information on how to access this file.

Oracle Database Solution Metrics

Examples of metrics available for the Oracle Database Solution include:

Oracle Database 8i, 9i, 10g

- Buffer Pool/Buffer Busy Wait Ratio (%)
- Buffer Pool/BUFFER_BUSY_WAIT (seconds)
- Buffer Pool/Hit Ratio (%)
- Buffer pool/IMMEDIATE_MISSES
- Buffer pool/MISSES
- Consistent changes
- Consistent gets
- Db block changes
- Db block gets

- DBWR buffers scanned
- DBWR checkpoints
- DBWR free buffers found
- DBWR lru scans
- DBWR make free requests
- DBWR summed scan depth
- Dictionary Cache/Miss Ratio (%)
- Dictionary Cache/TOTAL_GETS
- Dictionary Cache/TOTAL_MISSES
- Dispatcher busy rate - all networks
- Dispatcher busy rate - per network
- Dispatcher process queue avg. response time - per network
- Dispatcher process queue response time - all networks
- Latch Hit Ratio/Hit Ratio (%)
- Latch Hit Ratio/Hit Ratio (%)
- Library cache/IMMEDIATE_MISSES
- Library cache/MISSES
- Physical Blocks Read - for individual data file
- Physical Blocks Read per sec. - all data files
- Physical Blocks Written - for individual data file
- Physical Blocks Written per sec. - all data files
- Physical read time - for individual data file
- Physical Read Time (seconds) - all data files
- Physical Reads - for individual data file
- Physical Reads per sec. - all data files
- Physical write time - for individual data file
- Physical Write Time (seconds) - all data files

- Physical Writes - for individual data file
- Physical Writes per sec. - all data files
- Recursive calls
- Redo allocation/IMMEDIATE_MISSES
- Redo allocation/MISSES
- Redo buffer allocation retries
- Redo copy/IMMEDIATE_MISSES
- Redo copy/MISSES
- Redo entries
- Redo log space requests
- Redo synch writes
- Segment header/COUNT
- Sorts (disk)
- Sorts (memory)
- Table fetch by rowid
- Table fetch continued row
- Table scan blocks gotten
- Table scan rows gotten
- Table scans (long tables)
- Table scans (long tables)
- Table scans (short tables)
- Tablespaces w/ Less Than Two Free Extents/No. Tablespaces
- Total Latch Gets/Total Gets
- Total Latch Misses/Total Misses
- Total Latch Sleeps/Total Sleeps
- Undo header/COUNT
- Undo segment gets - for individual undo segment

- Undo segment waits - for individual undo segment
- Undo Segments/Total Gets - all undo segments
- Undo Segments/Total Waits - all undo segments
- User calls
- User commits
- User rollbacks

Oracle Database Solution Tools

The Oracle Solution Template deploys several tools that you can use to gather diagnostic information about an Oracle database. These tools are deployed to the same group as the monitors that are deployed by the solution template. They are displayed in much the same way as monitors but they are set as disabled. These tools are identified by the bold text Solution Tool in the Status field of the group content table. For more information, see "Understanding Oracle Database Solution Tools" on page 1119.

When the user clicks on one of these Solution Tools, SiteScope makes a custom SQL query to the database via the Database Connection Test tool. The results of the query are found in a table at the bottom of the page. From this page, the tool may be run as many times as necessary by clicking the Connect and Execute Query button. Bear in mind that some tools may incur substantial overhead on the database, so executing them in quick succession is not recommended.

Understanding Oracle Database Solution Tools

The Oracle Database Solution Tools are preconfigured diagnostic tool actions that are associated with and accessible to a particular Oracle Database Solution template deployment. These tools are deployed into the same group as the monitors that are deployed by the Oracle Database Solution template. The tools are listed in the monitor detail table and identified with the name Solution Tool in the Status field of the table.

Although the Solution tools are listed in the monitor table, they are not monitor instances. They do not run automatically, do not display a status based on action results, nor do they trigger alerts. They are preconfigured actions that make use of a SiteScope Diagnostic Tool to check certain statistics from the Oracle database that may indicate a performance problem.

Oracle Database Solution Tools

The following describes tools deployed as part of the Oracle Database Solution:

Oracle Solution Tool Name	Description and Usage Guidelines
Top Ten SQL Statements in Logical IOs Per Row	This tool performs a query which is designed to locate the most resource-intensive SQL statements being executed in the database. The V$SQL table is queried for the ten SQL statements which are performing the most logical IOs per row are displayed in a table. The statement IDs of these ten statements are displayed in a table, along with some additional resource-usage data for each statement. This additional data includes: ➤ **Physical IO Blocks.** The number of disk reads performed on behalf of the statement. ➤ **Logical IOs.** The number of buffer gets performed on behalf of the statement. ➤ **Rows Processed.** The number of rows processed when executing the statement. ➤ **Logical IOs Per Row.** The number of buffer gets performed per row that was processed when executing the statement. ➤ **Runs.** The number of executions of the statement. ➤ **Logical IOs Per Run.** The number of buffer gets per statement execution. **Note:** The action performed can have a significant impact on database resources and should not be executed frequently.
Number of Sessions Waiting Per Event	This tool can be used in troubleshooting stuck sessions. When several sessions become unresponsive, this tool can determine whether the stuck sessions are all waiting on the same event. The tool action displays a table containing the number of sessions waiting on specific events.

Oracle Solution Tool Name	Description and Usage Guidelines
Shared Server Process Contention (Common Queue Average Wait Time)	This tool calculates the average wait time of the shared server message queue (the Common Queue as recorded in V$QUEUE). A high average wait time may indicate contention between shared server processes.
Tablespaces With Less Than 2 Extents Available	This tool can be used to locate tablespaces which do not have enough adjacent free space to create more than two new extents. **Important:** This tool may not be useful on all Oracle configurations. For example, the query used by this tool (see below) would not work correctly on a database that uses dictionary-managed tablespaces (DMTs). Even for databases that used locally-managed tablespaces (LMTs), the query may not apply, depending on the segment space management scheme used for a specific tablespace. Tablespace management is a very complex subject. If there is any doubt as to the applicability of this tool to your specific Oracle installation, consult your local DBA and ask about the usefulness of the query used by this tool with respect to the target database configuration. The following query is executed by this tool: `SELECT owner, s.tablespace_name, segment_name, s.bytes, next_extent, MAX(f.bytes) largest FROM dba_segments s, dba_free_space f WHERE s.tablespace_name = f.tablespace_name(+) GROUP BY owner,s.tablespace_name,segment_name, s.bytes,next_extent HAVING next_extent*2>max(f.bytes)`

Use the following steps to run the Oracle Database Solution tools.

To run an Oracle Database Solution tool:

1. Click the group name for the group where the Oracle Solution monitors are deployed. The Group Detail page opens.
2. Find the Solution Tool for the action that you want to execute. See the **Name** column for the Solution Tool for a description of the action performed by that tool.
3. Click the **Tools** link to the right of the tool **Name** to execute the action. The Database Connection Test page opens. From this page, the tool may be run as many times as necessary by clicking the **Connect and Execute Query** button.

Note: Some Solution Tools may create significant overhead on the database depending on the query. Executing the tools in quick succession is therefore not advised.

The upper portion of the Database Connection Test page displays the database connection parameters used for the test. The results of the tool query are found in a table near the bottom of the page. Review the results based on the Description and Usage Guidelines for that tool.

61

SAP Solution Templates

To address the needs of SAP performance monitoring, HP offers SAP solution templates. The SiteScope SAP solution templates provide efficient and thorough monitoring of performance, availability, and usage statistics for SAP system components.

Understanding the SAP Solution

The SAP solution includes solution templates for the monitoring the following key SAP components:

- SAP CCMS
- SAP Java Web Application Server

The SAP Solution uses two solution templates which you use to deploy a collection of monitors configured with metrics to report on availability and performance. These monitoring configurations have been researched using best practice data and expertise from various sources.

Note: You must have the applicable SiteScope option license to use the SAP R/3 and SAP J2EE solution templates. Contact your HP sales representative for more information about licensing for solution templates.

The purpose of a solution template is to provide comprehensive SAP monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the SAP Solution templates include:

- Reduces the need for SAP server monitoring and performance domain expertise
- Reduces the time to configure and deploy multi-level monitoring for SAP servers
- Helps identify both real-time performance bottlenecks and longer term trends

You use the SAP R/3 solution template to deploy monitoring for SAP R/3 systems. You use the SAP J2EE template to monitor the SAP Java Web Application server if this component is deployed in the IT environment.

Using the SAP R/3 Solution Template

The SiteScope SAP R/3 solution template provides the tools you use to monitor the availability, usage statistics, and server performance statistics for SAP R/3 systems. This solution template deploys a set of monitors that test the health, availability, and performance of SAP R/3 servers.

System Requirements

Before you can use the SAP R/3 solution template, there are a number of configuration requirements involving the server environment. The following lists an overview of these requirements:

- SAP Java Connector libraries should be copied to the appropriate SiteScope folders.
- You need to know the user name and password that SiteScope must use to log into the SAP R/3 server.

For more information on system and configuration requirements, see "SAP CCMS Monitor Overview" on page 426. This monitor is deployed as part of the SAP R/3 solution template.

Deploying the SAP R/3 Solution Template

You use the following steps to deploy the SAP R/3 solution template.

To deploy the SAP R/3 Solution Template:

1. Right-click the SAP R/3 solution template icon to display the action menu and select **Copy**.
2. Select the monitor group container into which you want to deploy the SAP R/3 solution.
3. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
4. Complete the items on the SAP Solution Variable Values form as described in the section "SAP R/3 Solution Template Settings" below. When the required items are completed, click **OK**.

5 As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, click **Close**.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

SAP R/3 Solution Template Settings

The following describes the settings for the SAP R/3 solution:

Application Server

Enter the address of the SAP server you want to monitor.

SAP Client

Enter the Client to use for connecting to SAP.

System Number

Enter the System number for the SAP server.

Authentication User Name

Enter the user name required to connect to the SAP server.

Authentication Password

Enter the password required to connect to the SAP server.

Router String (Optional)

If you are connecting through a router, enter a router address string. You can locate 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 select **Properties** to view the router address. If you are not connecting through a router, leave this field blank.

Using the SAP J2EE Solution Template

The SiteScope SAP J2EE solution enables you to monitor the availability and server statistics for SAP Java Web application server clusters.

This solution template deploys a monitor that tests the health, availability, and performance of SAP Java Web application servers. You can use this solution template to deploy monitors for server-wide resources and metrics.

System Requirements

Before you can use the SAP J2EE solution template, there are a number of configuration requirements involving the server environment. The following lists an overview of these requirements:

- SAP Java Web application server libraries must be copied to the appropriate SiteScope folders.
- You must know the user name and password that SiteScope must use to log into the SAP Java Web application server.

For more information on system and configuration requirements, see “SAP Java Web Application Server Monitor Overview” on page 432. This monitor is deployed as part of the SAP J2EE solution template.

Deploying the SAP J2EE Solution Template

You use the following steps to deploy the SAP J2EE solution template.

To deploy a SAP J2EE solution template:

1. Right-click the SAP J2EE solution template icon to display the action menu and select **Copy**.
2. Select the monitor group container into which you want to deploy the SAP J2EE solution template.
3. Right-click on the container to display the action menu and select **Paste**. The Variable Values page opens in the contents panel.
4. Complete the items on the SAP Solution Variable Values page as described in the section "SAP J2EE Solution Template Settings" below. When the required items are completed, click the **OK** button.
5. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, click **Close**.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

SAP J2EE Solution Template Settings

The following describes the settings for the SAP J2EE Solution Template:

Application Server

Enter the address of the SAP Java Web Application Server you want to monitor.

Port

Enter the port number to use for connecting to the SAP server. The default port of 50004 is typically used.

Authentication User Name

Enter the user name required to connect to the SAP server.

Authentication Password

Enter the password required to connect to the SAP server.

62

Siebel Solution Templates

The SiteScope Siebel Solution templates provide efficient and thorough monitoring of performance, availability, and usage statistics for Siebel Application Server installed on Microsoft Windows and UNIX operating systems.

Understanding the Siebel Solution

The Siebel Solution includes solution templates for the monitoring the following key Siebel components:

- Siebel Application Server
- Siebel Gateway Server
- Siebel Web Server

The Siebel Solution uses three solution templates which you use to deploy a collection of monitors configured with metrics to report on availability and performance. These monitoring configurations have been researched using best practice data and expertise from various sources.

Note: You must have the applicable SiteScope option license to use the Siebel Solution templates. Contact your HP sales representative for more information about Solution licensing.

The purpose of a solution template is to provide comprehensive Siebel monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the Siebel Solution templates include:

- Reduces the need for Siebel server monitoring and performance domain expertise
- Reduces the time to configure and deploy multi-level monitoring for Siebel servers
- Helps identify both real-time performance bottlenecks and longer term trends

The primary solution template for Siebel is the Siebel Application Server template. This solution template is applicable to all Siebel deployments on Windows and UNIX platforms. You use this template to deploy monitoring for the core of the Siebel application. You use the Siebel Gateway Server and Siebel Web Server templates if these optional components are deployed in the IT environment.

Using the Siebel Application Server Solution Template

The SiteScope Siebel Application Server Solution Template provides tools you use to monitor the availability, usage statistics, and server performance statistics for Siebel Application servers installed on Windows and UNIX platforms. This solution template deploys a set of monitors that test the health, availability, and performance of Siebel Application Servers.

System Requirements

Before you can use the Siebel Application Server Solution Template, there are a number of configuration requirements involving the server environment. The following lists an overview of these requirements:

- The Siebel Server Manager client must be installed on the machine where SiteScope is running or accessible to the SiteScope machine. There are several options for how you can do this. See the documentation for the Siebel Server Manager Monitor for more information.
- You need to 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 need to know the fully qualified path to the client executable relative to that machine.
- You need to know the name of the Siebel applications that are available in your network. For example, call center, sales, and so on.
- You need to know the Siebel database connection URL and Database Driver.
- You need to know the user and password that SiteScope uses for logging into the Siebel server. This user must be granted Siebel Administrator responsibility on the Siebel server.
- You need to know a significant list of Siebel system component names and their corresponding aliases. See the section on the Settings in the Siebel Application Server Solution Form for a listing of component names and aliases.

See the sections on the “Siebel Web Server Monitor Overview” on page 441 and “Database Query Monitor Overview” on page 469 for more information on system and configuration requirements. These monitor types that are deployed as part of the Siebel Application Server Solution Template.

Deploying the Siebel Application Server Solution Template

You use the following steps to deploy the Siebel Application Server Solution Form.

To deploy the Siebel Application Server Solution Template:

1. Click on the SiteScope container into which you want to add the Siebel Solution and expand the container to display the group containers.
2. Right-click the Siebel Application Server Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the Siebel Application Server Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the Siebel Solution Variable Values form as described in the section “Siebel Application Server Solution Template Settings” below. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Siebel Application Server Solution Template Settings

The following describes the settings for the Siebel Application Server Solution:

SERVER_LIST

Select the machine name for the server where Siebel Application Server is running. Use the choose server to view the server selection page. Use the Server drop-down menu to select the server where the Siebel Application Server is running.

Application

Enter the Siebel Application Server machine name.

Enterprise

Enter the Siebel Enterprise server name.

Gateway

Enter the name of the Siebel Gateway server machine.

Server Logical Instance Name

Enter the Siebel server logical name.

Username

Enter the Siebel Client user name.

Password

Enter the password for the Siebel Client.

Server Manager Path

Enter the local path to the Siebel server manager client. For example: D:\sea703\client\bin.

Siebel Disk

Enter the disk name where Siebel is installed.

Siebel Root Dir

Enter the path of the shared Siebel root directory. For example, the shared root directory for a Siebel 7.5.2 server would be: sea752.

Siebel Database Machine Name

Enter the Siebel database machine name.

Database Connection URL

Enter the URL to the database connection. For example, if the ODBC connection is called test, the URL would be jdbc:odbc:test.

Enter the connection URL to the database you want to connect to. The syntax is jdbc:oracle:thin:@<server name or ip address>:<database server port>:<sid>.

For example, to connect to the ORCL database on a machine using port 1521 you would use:

jdbc:oracle:thin:@206.168.191.19:1521:ORCL.

Note: The colon and @ symbols must be included as shown.

Database Driver

Enter the driver used to connect to the database.

Database Username

Enter the user name SiteScope should use to access the Siebel database.

Database Password

Enter the password for the user name used to access the Siebel database.

CG Callcenter Name

Enter the Siebel CallCenter component group name.

CG Callcenter Alias

Enter the Siebel CallCenter component group alias.

CG System Management Name

Enter the Siebel System Management component group name.

CG System Management Alias

Enter the Siebel System Management component group alias.

CP Callcenter Name

Enter the Siebel CallCenter component name.

CP Callcenter Alias

Enter the Siebel CallCenter component alias.

CP eService Name

Enter the Siebel eService component name.

CP eService Alias

Enter the Siebel eService component alias.

CP Srvr Request Broker Name

Enter the Siebel Server Request Broker component name.

CP Srvr Request Broker Alias

Enter the Siebel Server Request Broker component alias.

CP_Srvr_Request_Processor_Name

Enter the Siebel Server Request Processor component name.

CP Srvr Request Processor Alias

Enter the Siebel Server Request Processor component alias.

CP Server Manager Name

Enter the Siebel Server Manager component name.

CP Server Manager Alias

Enter the Siebel Server Manager component alias.

CP File System Manager Name

Enter the Siebel File System Manager component name.

CP File System Manager Alias

Enter the Siebel File System Manager component alias.

CP Client Administration Name

Enter the Siebel Client Administration component name.

CP Client Administration Alias

Enter the Siebel Client Administration component alias.

Siebel Application Server Solution Metrics

The following metrics are available for the Siebel Application Server Solution:

- Component Objects/Siebel Call Center/Call Center Object Manager
  - Average Response Time
  - Average Think Time
  - Avg SQL Execute Time
  - CP_DISP_RUN_STATE
  - CP_DISP_RUN_STATE
  - Max %CPU Time
  - Max Memory Used
  - No. of Running Instances
  - No. of tasks in error
  - Tasks Exceeding Configured Cap
- Component Stats/Siebel Call Center/eService Object Manager
  - Average Response Time
  - Average Think Time
  - Avg SQL Execute Time
  - Max %CPU Time
  - Max Memory Used
  - No. of Running Instances
  - No. of tasks in error
  - Tasks Exceeding Configured Cap

- Component Objects/System Management/Server Request Broker
  - Avg SQL Execute Time
  - CP_DISP_RUN_STATE
  - Max %CPU Time
  - Max Memory Used
  - No. of Running Instances
  - No. of tasks in error
  - Tasks Exceeding Configured Cap
- Component Objects/System Management/Server Request Processor
  - Avg SQL Execute Time
  - CP_DISP_RUN_STATE
  - Max %CPU Time
  - Max Memory Used
  - No. of Running Instances
  - No. of tasks in error
  - Tasks Exceeding Configured Cap
- Component Objects/System Management/Server Manager
  - Avg SQL Execute Time
  - CP_DISP_RUN_STATE
  - Max %CPU Time
  - Max Memory Used
  - No. of Running Instances
  - No. of tasks in error
  - Tasks Exceeding Configured Cap

- Component Objects/System Management/File System Manager
  - Avg SQL Execute Time
  - CP_DISP_RUN_STATE
  - Max %CPU Time
  - Max Memory Used
  - No. of tasks in error
  - Running Instances
  - Tasks Exceeding Configured Cap
- Component Objects/System Management/Client Administration
  - Avg SQL Execute Time
  - CP_DISP_RUN_STATE
  - Max %CPU Time
  - Max Memory Used
  - No. of Running Instances
  - No. of tasks in error
  - Tasks Exceeding Configured Cap
- CPU utilization
- Database query - transaction logging process
- Database query - workflow rules process
- Database query - transaction router process
- Database query - enterprise integration manager process
- Directory (Checks Siebel Server LOG and \DOCKING\TXNPROC directory) for:
  - # of files
  - Size in MB
  - Time since last modified
- Disk space - % full

- Log file - siebsrvr\LOG files
- Log file - SCCObjMgr_enu log files
- Max % CPU time - Server Processes/Siebel Components (SIEBMTSH / SIEBMTSHMW)
- Max % CPU time - Server Processes/Siebel Background Tasks (SIEBPROC / SIEBSH)
- Max % CPU time - Server Processes/Siebel SrvrMgr Session (SIEBSESS)
- Max Memory Used - Server Processes/Siebel Background Tasks (SIEBPROC / SIEBSH)
- Max Memory Used - Server Processes/Siebel Application Server Process (SIEBSVC)
- Max Memory Used - Server Processes/Siebel SrvrMgr Session (SIEBSESS)
- Memory - % used
- Memory - MB free
- Number of running instances - Server Processes/Siebel Components (SIEBMTSH / SIEBMTSHMW
- Number of running instances - Server Processes/Siebel Background Tasks (SIEBPROC / SIEBSH
- Number of running instances - Server Processes/Siebel SrvrMgr Session (SIEBSESS)
- Number of running instances - Server Processes/Siebel Application Server Process (SIEBSVC)
- Ping (availability test for the Siebel App Server)
- Service (checks Siebel Server service test)

Using the Siebel Gateway Server Solution Template

The SiteScope Siebel Gateway Server Solution allows you to monitor the availability and server statistics for Siebel Gateway servers installed on Windows and UNIX platforms.

This solution template deploys a set of monitors that test the health, availability, and performance of Siebel Gateway Servers. You can use this solution template to deploy monitors for server-wide resources and metrics.

Deploying the Siebel Gateway Server Solution Template

You use the following steps to deploy the Siebel Gateway Server Solution Template.

To deploy a Siebel Gateway Server Solution Template:

1. Click on the SiteScope container into which you want to add the Siebel Solution and expand the container to display the group containers.
2. Right-click the Siebel Gateway Server Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the Siebel Gateway Server Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the Siebel Solution Variable Values form as described in the section “Siebel Gateway Server Solution Template Settings” below. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

   As the monitors are created, the monitor type and name are displayed along with messages of any errors found. A "success" message is shown if the monitors are created successfully. The process does not run the monitor.

After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Siebel Gateway Server Solution Template Settings

The following describes the settings for the Siebel Gateway Server Solution:

SERVER_LIST

Enter the name of the server where the Siebel Gateway Server is running. Do NOT enter backslashes (\\) that indicate a UNC path as part of the name of the server.

Siebel Disk

Enter the disk drive where the Siebel gateway server is running.

Siebel Directory

Enter the path to the Siebel Directory. This directory should contain at least an Admin Console installation.

Siebel Logical Instance Name

Enter the Siebel server logical name value (for UNIX only).

Siebel Gateway Server Solution Metrics

The following metrics are available for the Siebel Gateway Server Solution:

- CPU utilization
- Disk space - % full
- Disk space - MB free
- Disk space - total disk
- Directory (# of files in gtwysrvr\LOG directory)
- Memory - % used
- Memory - MB free
- Memory - pages/sec.
- Service - Siebel Gateway Name Server Service

Using the Siebel Web Server Solution Template

The SiteScope Siebel Web Server Solution allows you to monitor the availability and server statistics for Siebel Web servers installed on Windows and UNIX platforms. This solution template deploys a set of monitors that test the health, availability, and performance of Siebel Web Servers.

System Requirements

Before you can use the Siebel Solution, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the machine where the Siebel Web Server is running.
- Siebel Web Server Solution is designed for use with Siebel running on Microsoft Windows platforms.
- Template assumes that the Siebel Web Server is running on Microsoft Internet Information Server (IIS).

Deploying the Siebel Web Server Solution Template

You use the following steps to deploy the Siebel Web Server Solution Template.

To deploy a Siebel Web Server Solution Template:

1. Click on the SiteScope container into which you want to add the Siebel Solution and expand the container to display the group containers.
2. Right-click the Siebel Web Server Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the Siebel Web Server Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the Siebel Solution Variable Values form as described in the section “Siebel Web Server Solution Template Settings” below. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

   After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note: Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

Siebel Web Server Solution Template Settings

The following describes the settings on the Siebel Web Server Solution Form:

SERVER_LIST

Select the Siebel Web server machine name. Use the choose server to view the server selection page. Use the Server drop-down menu to select the server where the Siebel Web server is running.

Siebel Root Dir

Enter the name of the shared Siebel root directory. For example Siebel root directory on Windows: `sea752`.

Siebel Disk

Enter the disk name or drive letter where the Siebel Web server is installed.

Siebel Logical Instance Name

Enter the Siebel server logical name (for UNIX only).

Application

Enter the Siebel application to monitor. For example: callcenter_enu. Consult with your Siebel administrator for information on names of the installed Siebel applications.

Username

Enter the Siebel Client user name needed to log into the Siebel Web server.

Password

Enter the Siebel Client password needed to log into the Siebel Web server.

Siebel Web Server Solution Metrics

The following metrics are available for the Siebel Web Server Solution:

- CPU utilization
- Directory (# of files in SWEApp\LOG directory)
- Disk space - % full
- Disk space - MB free
- Disk space - total disk
- Memory - $ used
- Memory - MB free
- Port - monitors port 80
- Service - IIS Admin Service
- Siebel Applications/callcenter_enu/Frequency mean
- Siebel System Stats/Request Time/Frequency mean
- URL (http://testwin2k14/callcenter_enu/start.swe?SWECmd=Start)
- URL of web plug-in server stats page
- Siebel Applications/callcenter_enu/Frequency mean
- Siebel System Stats/Request Time/Frequency mean
- Web Service - Bytes Received/sec
- Web Service - Bytes Sent/sec
- Web Service - Bytes Total/sec
- Web Service -- Current Connections
- Web Service - Current Non Anonymous Users
- Web Service - Get Requests/sec
- Web Service - Maximum Connections
- Web Service - Post Requests/sec
- Web Service - Total Not Found Errors

63

Solaris Host Solution Templates

The Solaris Host Solution Template allows you to monitor any host which runs a supported version of a Solaris operating system. This solution gathers generic metrics that represent the health, availability and performance of the target Solaris machine.

Understanding the Solaris Host Solution

This solution is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the Solaris host. The template supports the versions of Solaris that are supported by SiteScope. For details, see “System Requirements” in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can generate a Server Centric Report which displays data from three different metrics about the server being monitored. It is recommended to use Solution Templates when creating the UNIX Resource Monitor, since the appropriate monitors and metrics are already configured. For more information on generating a Server Centric Report, see “Generating a Server Centric Report” on page 337.

Note: You must have the applicable SiteScope option license to use the Solaris Host Solution Template. Contact your HP sales representative for more information about Solution licensing.

The Solaris Host Solution Template provide comprehensive Solaris operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the Solaris Host Solution Template include:

- Reduces the need for Solaris performance domain expertise
- Reduces the time to configure and deploy various performance monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds only negligible overhead to production systems

The Solaris Host solution Template deploys monitors that target the following aspects of Solaris performance and health:

- CPU status and utilization details
- Memory status and utilization details
- File system status and utilization details

An in depth description of the Solaris Host Solution settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_OS_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

System Requirements

The Solaris Host Solution license must be applied to the SiteScope server onto which you want to deploy the Solaris Host Solution. See "SiteScope General Preferences" on page 226 for details on how to enter license information.

Before you can use the Solaris Host Solution Template, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the target Solaris host.
- The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test. For details, See "UNIX Remote Preferences Overview" on page 201.
- The SiteScope server itself can also be monitoring if it runs a supported Solaris operating system.
- The template supports the Solaris versions supported by SiteScope. For details, see "System Requirements" in the *HP SiteScope Deployment Guide* PDF.

Deploying the Solaris Solution Template

Deploy one Solaris Solution Template for each Solaris server in your environment. Use the following steps to deploy a Solaris Host Solution Template.

To deploy a Solaris Host Solution Template:

1. Click the SiteScope container into which you want to add the Solaris Host Solution and expand the container to display the group containers.
2. In the left tree, expand **Solution Templates**.
3. Right-click the **Solaris Host** solution template to display the action menu and select **Copy**.
4. Select the SiteScope container or the monitor group container into which you want to deploy the solution template.
5. Right-click the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.

6 In the **SERVER_LIST** list-box, select the Solaris remote for which you want to deploy the solution. You can also deploy on the SiteScope server by selecting **SiteScope Server** in the list-box. Click the **OK** button.

7 If some of the monitors failed to deploy, a paste results message is shown listing the names of the monitors created along with messages describing the error. After viewing the message, select **Close**.

Deploying the Solaris Host Solution Template creates a new monitor group container in which the individual solution monitors are added. The monitor group container is assigned a name in the format Solaris monitors for <server_name> where server_name is the server selected from the **Server_List** field.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution Templates do not configure any automated alerts or reports for the monitors created. You may create and associate one or more alert definitions or reports to the monitors or monitor groups created by solution templates.
- The Solaris Host Solution Template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Service Centric Report support.

64

WebLogic Solution Template

To address the needs of WebLogic performance monitoring, HP offers the WebLogic Solution. The SiteScope WebLogic Solution template provides efficient and thorough monitoring of performance, availability, and usage statistics for BEA WebLogic 6.x, 7.x, 8.x, and 9.x application servers.

Understanding the WebLogic Solution

This solution uses a template which you can use to deploy a collection of WebLogic Monitors configured with default metrics. The WebLogic Solution monitor deployment process is highly customizable in that it allows the user to select the specific J2EE components on an application server which SiteScope should actively monitor.

Note: You must have the applicable SiteScope option license to use the WebLogic Solution Template. Contact your HP sales representative for more information about Solution licensing.

The purpose of a solution template is to provide comprehensive WebLogic monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

An in depth description of the WebLogic Solution is available in the SiteScope WebLogic Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_WebLogic_Best_Practices.pdf**. This is a password protected document. The password is provided along with the WebLogic Solution license key from HP.

Benefits of the WebLogic Solution Template include:

- Reduces the need for WebLogic performance domain expertise
- Reduces the time to configure and deploy WebLogic monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds no overhead to production systems

The WebLogic Solution Template deploys monitors that target the following aspects of WebLogic performance and health:

Server Performance Statistics

This category refers to a collection of server-wide resources that are exposed through the management interface of a WebLogic Application Server.

Application Performance Statistics

Metrics for all of your deployed applications, EJBs, web applications, and servlets are available for monitoring through the WebLogic Solution. The user is responsible for selecting which of these J2EE components he would like to have monitors automatically deployed for. A set of metrics based on WebLogic best practices are monitored for each selected J2EE component.

WebLogic Solution Metrics

Some of the components that can be monitored with this solution include:

EJB Pool Runtime

- Access Total Count
- Beans In Use Count
- Beans In Use Current Count
- Destroyed Total Count
- Idle Beans Count
- Miss Total Count
- Pooled Beans Current Count
- Timeout Total Count
- Timeout Total Count
- Waiter Current Count
- Waiter Total Count

EJB Transaction Runtime

- Transactions Committed Total Count
- Transactions Rolled Back Total Count
- Transactions Timed Out Total Count

EJB Cache Runtime

- Activation Count
- Cache Access Count
- Cache Hit Count
- Cache Miss Count
- Cached Beans Current Count
- Passivation Count

Server Runtime

- Activation Time
- Admin Server Listen Port
- Listen Port
- Restarts Total Count
- Sockets Opened Total Count

Servlet Runtime

- Execution Time Average
- Execution Time High
- Execution Time Low
- Execution Time Total
- Invocation Total Count
- Pool Max Capacity
- Reload Total Count

Web App Component Runtime

- Open Sessions Current Count
- Open Sessions High Count
- Sessions Opened Total Count

JTA Runtime

- Seconds Active Total Count
- Transaction Committed Total Count
- Transaction Heuristics Total Count
- Transaction Rolled Back App Total Count
- Transaction Rolled Back Resource Total Count
- Transaction Rolled Back System Total Count
- Transaction Rolled Back Timeout Total Count

- Transaction Rolled Back Total Count
- Transaction Total Count

JVM Runtime

- Heap Free Current
- Heap Size Current

JDBC Connection Pool Runtime

- Active Connections Current Count
- Active Connections High Count
- Connection Delay Time
- Connections Total Count
- Max Capacity
- Wait Seconds High Count
- Waiting For Connection Current Count
- Waiting For Connection High Count

Execute Queue Runtime

- Execute Thread Current Idle Count
- Pending Request Oldest Time
- Serviced Request Total Count
- Pending Request Current Count

Cluster Runtime

- Alive Server Count
- Foreign Fragments Dropped Count
- Fragments Received Count
- Fragments Sent Count
- Multicast Messages Lost Count

- Primary Count
- Resend Requests Count

Log Broadcaster Runtime

- Messages Logged

Using the WebLogic Solution Template

This solution template deploys a set of monitors that test the health, availability, and performance of a WebLogic Application Server and its deployed applications and components. The deployed monitors check server-wide statistics such as memory usage, as well as metrics specific to individual J2EE components, such as the number of activates and passivates of a particular EJB.

Usage Guidelines

Use the WebLogic Solution to monitor statistics from WebLogic 6.x, 7.x, 8.x, and 9.x servers. This solution automatically creates several groups by default which monitor important application server metrics, but it also provides a user interface that allows you to select all or some of the individual components that are available for monitoring.

The WebLogic Solution Template deploys a WebLogic Application Server Monitor for each module that is selected from the user interface. This monitor uses the Java JMX interface to access Runtime MBeans on the WebLogic server. An MBean is a container that holds the performance metrics. You may need to set certain permissions on the WebLogic server for SiteScope to be able to monitor MBeans. For an overview on configuring access to WebLogic servers for SiteScope monitors, see “WebLogic Application Server Monitor Overview” on page 448.

Deploying the WebLogic Solution Template

You use the following steps to deploy the WebLogic Application Server Solution Form.

To deploy a WebLogic Solution Template:

1. Click on the SiteScope container into which you want to add the WebLogic Solution and expand the container to display the group containers.
2. Right-click the WebLogic Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the WebLogic Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the WebLogic Solution Variable Values form as described in the section “WebLogic Solution (versions 6.x, 7.x, 8.x) Template Settings” below. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

   After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

WebLogic Solution (version 9.x) Template Settings

The following describes the settings for the WebLogic Application Server Solution:

WEBLOGIC9_URL

Enter the URL for the WebLogic Application Server 9.x. The default is:

```
service:jmx:rmi:///jndi/iiop://<local host>:7001/
weblogic.management.mbeanservers.runtime
```

where <local host> is the name of the machine running WebLogic Application Server 9.x.

WebLogic Solution (versions 6.x, 7.x, 8.x) Template Settings

The following describes the settings for the WebLogic Application Server Solution:

Timeout

Enter the number of seconds to wait for a data request to arrive at the WebLogic server. The default is 180.

Port Number

Enter the port number that the WebLogic server is responding on. The default port is 7001.

Password

Enter the password required to log into the WebLogic server.

User Name

Enter the user name required to log into the WebLogic server.

Server

Enter the name or address of the server where WebLogic is running.

WebLogic Jar File

Enter the absolute path name 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. An example is: c:\bea\weblogic7\ebcc\lib\ext\weblogic.jar.

This file is not 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.

Note: Do not install weblogic.jar in the SiteScope directory tree. For example, do not install it in the <SiteScope install path>/SiteScope/java/lib/ext directory as this causes the WebLogic monitors to fail. You must create a separate directory on the server where SiteScope is running for this file.

Selecting Modules for Monitoring

The WebLogic Solution presents a hierarchical list from which the user can select the modules to deploy WebLogic Monitors against. This list is broken down into two main sections:

- per-server resources
- J2EE components organized by application

Some of the modules in these categories are automatically selected by default because they represent critical components in the system (for example, the JVM statistics for the application server). The remainder of the modules are not automatically selected. This allows the user to customize the deployment of this solution to focus on one application, a particular type of EJB, a set of servlets and web applications, or some other aspect of the application server.

For the most part, the organization of this list of modules is intuitive. The hierarchy of applications, EJBs, web applications, and servlets is very similar to the organization of these entities in the WebLogic Administration Console. In almost every case, selecting a module causes a monitor with all relevant metrics to be deployed against that part of the WebLogic server. However, when selecting EJBs to monitor, you notice that they are broken down according to three types of metrics: Pool, Transaction, and Cache. The reason for this is twofold: (1) it is more useful to be able to monitor one aspect of a particular EJB instead per WebLogic Monitor for purposes of alerting and organization, and (2) not all three of these types of metrics are available for all EJBs.

Below is a brief description of the metrics that are monitored for each type of EJB monitoring:

- **Per-EJB Transaction Statistics.** This category of EJB monitor contains metrics related to transactions made for the EJB. These metrics include the number of transactions rolled back, the number of transactions that timed out, and the number of transactions that were successfully committed.
- **Per-EJB Pool Statistics.** This category of EJB monitor contains metrics related to the pool for the EJB. When the user selects an EJB under this heading, many useful metrics are monitored, including the number of times an attempt to get a bean instance from the pool failed, the number of current available instances in the pool, the number of threads currently waiting for an instance, and the number of times a bean instance was destroyed due to a non-application exception.
- **Per-EJB Cache Statistics.** The cache statistics include any metrics relating to the caching of the particular EJB. Metrics like the number of cache hits and misses, and the number of activates and passivates of the EJB are monitored when an EJB under this heading is selected for monitoring.

When you have finished making your module selections in the popup window, scroll to the bottom of the Module Selection window and click the Select Modules button. This updates the main browser window with a list of the modules you selected. You can then review your selections and remove any modules that you don't want a monitor to be created for.

When you are satisfied with the list of selected modules in the main browser window, you may hit the Submit button to proceed to the next step in deploying the WebLogic Solution.

65

WebSphere Solution Template

To address the needs of WebSphere performance monitoring, HP offers the WebSphere Solution. The SiteScope WebSphere Solution provides efficient and thorough monitoring of performance, availability, and usage statistics for IBM WebSphere Application Server 5.x and 6.x.

Understanding the WebSphere Solution

This solution uses a template you can use to deploy a collection of WebSphere Monitors configured with default metrics. The WebSphere Solution monitor deployment process is highly customizable in that it allows the user to select the specific J2EE components on an application server which SiteScope should actively monitor.

Note: You must have the applicable SiteScope option license to use the WebSphere Solution templates. Contact your HP Sales representative for more information about Solution licensing.

The purpose of a solution template is to provide comprehensive WebSphere monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

An in depth description of the WebSphere Solution is available in the SiteScope WebSphere Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_WebSphere_Best_Practices.pdf**. This is a password protected document. The password is provided along with the WebSphere Solution license key from HP.

Benefits of the WebSphere solution template include:

- Reduces the need for WebSphere performance domain expertise
- Reduces the time to configure and deploy WebSphere monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds no overhead to production systems

The WebSphere Solution Template deploys monitors that target the following aspects of WebSphere performance and health:

Server Performance Statistics

This category refers to a collection of server-wide resources that are exposed through the management interface of a WebSphere Application Server.

Application Performance Statistics

Metrics for all of your deployed applications, EJBs, web applications, and servlets are available for monitoring through the WebSphere Solution. The user is responsible for selecting which of these J2EE components he would like to have monitors automatically deployed for. A set of metrics based on WebSphere best practices are monitored for each selected J2EE component.

WebSphere Application Server Solution Metrics

Some of the components and metrics that can be monitored with this solution include:

EJB General

- Active Methods
- Avg. Method Rt (ms)
- Concurrent Lives
- Num Destroys
- Num Instantiates
- Total Method Calls

Entity EJB Performance

- Active Methods
- Avg Drain Size
- Avg Method Rt
- Concurrent Lives
- Drains From Pool
- Gets Found
- Gets From Pool
- Num Activates
- Num Creates
- Num Destroys
- Num Instantiates
- Num Loads
- Num Passivates
- Num Removes
- Num Stores

- Pool Size
- Returns Discarded
- Returns To Pool
- Total Method Calls

Stateful Session EJB Performance

- Active Methods
- Avg Method Rt
- Concurrent Lives
- Num Activates
- Num Creates
- Num Destroys
- Num Instantiates
- Num Passivates
- Num Removes
- Total Method Calls

Stateless Session EJB Performance

- Active Methods
- Avg Drain Size
- Avg Method Rt
- Concurrent Lives
- Drains From Pool
- Gets Found
- Gets From Pool
- Num Destroys
- Num Instantiates
- Pool Size

- Returns Discarded
- Returns To Pool
- Total Method Calls

Message Driven EJB Performance

- Active Methods
- Avg Drain Size
- Avg Method Rt
- Concurrent Lives
- Drains From Pool
- Gets Found
- Gets From Pool
- Num Destroys
- Num Instantiates
- Pool Size
- Returns Discarded
- Returns To Pool
- Total Method Calls

Database Connections

- Avg. Wait Time (ms)
- Concurrent Waiters
- Faults
- Num allocates
- Num Creates
- Num Destroys
- Num returns
- Percent Maxed

- Percent Used
- Pool Size
- PrepStmt Cache Discards

JVM Runtime

- Free Memory (bytes)
- Total Memory (bytes)
- Used Memory (bytes)

Servlet Session Manager

- Active Sessions
- Created Sessions
- Invalidated Sessions
- Live Sessions
- Session Lifetime

ORB Container Thread Pool

- Active Threads
- Active Threads
- Percent Maxed
- Percent Maxed
- Pool Size
- Pool Size
- Thread Creates
- Thread Creates
- Thread Destroys
- Thread Destroys
- Web Container Thread Pool

Transaction Manager

- Active Global Trans
- Active Local Trans
- Global Before Completion Duration
- Global Commit Duration
- Global Prepare Duration
- Global Trans Begun
- Global Trans Committed
- Global Trans Duration
- Global Trans Involved
- Global Trans RolledBack
- Global Trans Timeout
- Local Before Completion Duration
- Local Commit Duration
- Local Trans Begun
- Local Trans Committed
- Local Trans Duration
- Local Trans RolledBack
- Local Trans Timeout
- Num Optimizations

Web Applications

- Concurrent Requests
- Num Errors
- Num Loaded Servlets
- Num Reloads

- Response Time (ms)
- Total Requests

Servlets

- Concurrent Requests
- Num Errors
- Response Time
- Total Requests

Using the WebSphere Solution Template

The SiteScope WebSphere Application Server Solution allows you to monitor the availability, server statistics, and deployed J2EE components on a IBM WebSphere Application Server 5.x or 6.x.

Usage Guidelines

This solution template deploys a set of monitors that test the health, availability, and performance of IBM WebSphere 5.x Application Servers. It uses the IBM JMX interface to the Performance Monitoring Infrastructure of WebSphere. You can use this solution template to deploy monitors for server-wide resources and metrics (for example, thread pool and JVM metrics). You can also create monitors for the deployed EJBs, Web Applications, and Servlets using this solution template. For details, see "Understanding the WebSphere Solution" on page 1165.

System Requirements

Before you can use the WebSphere Solution, there are a number of configuration requirements involving the server environment. For an overview of these requirements, see "WebSphere Application Server Monitor Overview" on page 451.

Deploying the WebSphere Solution Template

You use the following steps to deploy the WebSphere Application Server Solution.

To deploy a WebSphere Solution Template:

1. Click on the SiteScope container into which you want to add the WebSphere Solution and expand the container to display the group containers.
2. Right-click the WebSphere Solution template icon to display the action menu and select **Copy**.
3. Select the SiteScope container or the monitor group container into which you want to deploy the WebSphere Solution.
4. Right-click on the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.
5. Complete the items on the WebSphere Solution Variable Values form as described in the section “WebSphere Solution Template Settings” on page 1174. When the required items are completed, click the **OK** button.
6. As SiteScope creates the monitors, a paste results message is shown listing the names of the monitors created along with messages indicating success or error. After the monitors have been created, select **Close**.

   After deploying the monitors, you should review the Error and Warning status thresholds and adjust them according to the importance of the monitored element. You should also create alerts and associate them to the newly created monitors to provide notification when an error is detected.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution Templates do not configure any automated alerts for the monitors created. You must create and associate one or more alert definitions to the monitors or monitor groups created by solution templates.

WebSphere Solution Template Settings

The following describes the settings on the WebSphere Application Server Solution Form:

WebSphere Directory

Enter the path to the WebSphere directory that contains the /java and /lib subdirectories from the WebSphere Application Server.

In WebSphere 6.x, this directory must also contain /profiles subdirectory. This subdirectory has all Key Store and Trust Store files needed for Global Security. The server profile in /profiles subdirectory must be called **default**. If the server profile has a different name, rename it to **default**.

WebSphere User Name

Enter the user name that SiteScope should use to login to WebSphere Application server.

In WebSphere 6.x, Global Security is not supported in the solution template. This means that you can type in any text however, the text box cannot be left empty. If you need to work with Global Security, complete this template. Edit the WebSphere monitor and, in the Advanced Settings pane, update the Global Security fields (Trust Store, Trust Store Password, Key Store, Key Store Password).

WebSphere Port

Enter the port number of the WebSphere server. This should be the SOAP port for WebSphere 5.x. The default port number is 8880.

WebSphere Password

Enter the password that SiteScope should use to login to WebSphere server.

In WebSphere 6.x, Global Security is not supported in the solution template. This means that you can type in any text however, the text box cannot be left empty. If you need to work with Global Security, complete this template. Edit the WebSphere monitor and, in the Advanced Settings pane, update the Global Security fields (Trust Store, Trust Store Password, Key Store, Key Store Password).

WebSphere Client Properties File

Enter the client properties file. The default is **/properties/soap.client.props**.

WebSphere Server

Enter the name of the server where the WebSphere Application is running. Do not enter backslashes (\\) that indicate a UNC path as part of the name of the server.

66

Windows Host Solution Template

The Windows Host Solution template allows you to monitor any host which runs a supported version of a Windows operating system. This solution gathers generic metrics that represent the health, availability, and performance of the target Windows machine.

Understanding the Windows Host Solution

This solution is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the host. The template supports Windows 2000, Windows XP, and Windows Server 2003.

For Windows Resource Monitors, you can generate a Server Centric Report which displays data from three different metrics about the server being monitored. It is recommended to use Solution Templates when creating the Windows Resource Monitor, since the appropriate monitors and metrics are already configured. For more information on generating a Server Centric Report, see “Generating a Server Centric Report” on page 337.

Note: You must have the applicable SiteScope option license to use the Windows Host Solution template. Contact your HP sales representative for more information about Solution licensing.

The Windows Host Solution template provides comprehensive Windows operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application.

Benefits of the Windows Host Solution template include:

- Reduces the need for Windows performance domain expertise
- Reduces the time to configure and deploy various performance monitors
- Helps identify both real-time performance bottlenecks and longer term trends
- Adds only negligible overhead to production systems

The Windows Host solution template deploys monitors that target the following aspects of Windows performance and health:

- High-level CPU status and utilization details
- High-level Memory status and utilization details
- Disk utilization information

An in depth description of the Windows Host Solution settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_OS_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

System Requirements

The Windows Host Solution license must be applied to the SiteScope server onto which you want to deploy the Windows Host Solution. See the section on "SiteScope General Preferences" on page 226 for details on how to enter license information.

Before you can use the Windows Host Solution, there are a number of configuration requirements involving the server environment:

- SiteScope server must be able to connect to the target Windows host. Use the Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Windows Resource monitor may require special configuration. For details, see "Windows Resources Monitor Overview" on page 544.
- The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test. Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, See "Configure SiteScope to Monitor a Remote Windows Server" on page 218.
- The SiteScope server itself can also be monitoring if it runs a supported Windows operating system.
- The template supports Windows 2000, Windows XP, and Windows Server 2003.

Deploying the Windows Solution Template

Deploy a Windows Solution Template for each Windows server in your environment. Use the following steps to deploy a Windows Host Solution Template.

To deploy a Windows Host Solution Template:

1. Click the SiteScope container into which you want to add the Windows Host Solution and expand the container to display the group containers.
2. In the left tree, expand **Solution Templates**.
3. Right-click the **Windows Host** solution template icon to display the action menu and select **Copy**.

4 Select the SiteScope container or the monitor group container into which you want to deploy the Windows Host Solution.

5 Right-click the container to display the action menu and select **Paste**. The Variable Values form opens in the contents panel.

6 In the **SERVER_LIST** list-box, select the Windows remote machines for which you want to deploy the solution. You can also deploy on the SiteScope server by selecting **SiteScope Server** in the list-box. Click the **OK** button.

7 If some of the monitors failed to deploy, a paste results message is shown listing the names of the monitors created along with messages describing the error. After viewing the message, select **Close**.

Deploying the Windows Host Solution creates a new monitor group container in which the individual solution monitors are added. The monitor group container is assigned a name in the format Windows monitors for <server_name> where server_name is the server selected from the **Server_List** field.

Note:

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- Solution Templates do not configure any automated alerts or reports for the monitors created. You may create and associate one or more alert definitions or reports to the monitors or monitor groups created by solution templates.
- The Windows Host Solution deploys a Windows Resource Monitor for each target host. This monitor is an additional monitor that is required for Service Centric Report support.

Part VII

Alerts and Reports

67

SiteScope Alerts

This chapter describes SiteScope Alerts.

Understanding Alerts

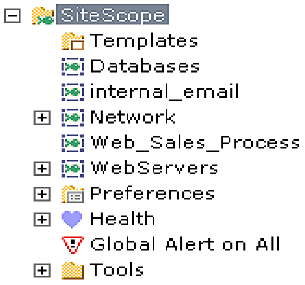
SiteScope alerts are types of notification actions that SiteScope can execute. Alerts are triggered or executed when the conditions for the alert definition are detected. Normally, you use an alert to send some notification of an event or change of status in some element or system in your infrastructure. For example, an alert can be triggered when a SiteScope monitor detects a change from Good to Error indicating that the monitored system has stopped responding.

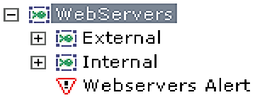
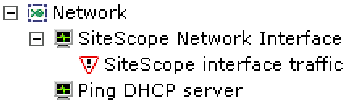
You can also have SiteScope respond to problems by automatically initiating recovery or action scripts with Script Alert. For example, you can configure a Script Alert to execute a script to restart a server if a monitor detects that a system is no longer responding and CPU utilization has reached 100%.

Alert definitions are indicated by the icon in the monitor tree. An alert definition contains settings that tell SiteScope what monitors can trigger the alert, what condition to watch for, and what information to send. The type of action is set by the alert type. For example, you can create an alert that includes instructions for SiteScope to send the specific server address and error code to your pager or e-mail when an error condition is detected on a particular system.

SiteScope alerts can be configured in several ways. Alerts can be associated explicitly with one or more individual monitors, with one or more groups of monitors, a combination of monitors and groups, or globally for all monitors on a particular installation of SiteScope. Global and group-wise alerting is generally the most efficient but may not provide the needed control. You can use the **Filter Settings** feature on each alert definition page to create filter criteria to control global and group alerts to more specific criteria. Filter criteria can be used to restrict the alert to only monitors of a certain type, that contain a certain text string or other filter criteria. For example, creating a global alert with a filter criteria for CPU Monitor creates an alert that is only triggered for CPU monitor types.

The table below shows an overview of the different alert types, associations, and considerations.

Alert Class	Description
Global Alerts	Alerts that are triggered when any monitor on a given SiteScope reports the category status defined for the alert. New groups and monitors added after the alert definition is created are automatically associated with the alert. The following display is an example of a global alert associated with the SiteScope node. All monitors can trigger this alert.  ⊟ SiteScope Templates Databases internal_email ⊞ Network Web_Sales_Process ⊞ WebServers ⊞ Preferences ⊞ Health Global Alert on All ⊞ Tools **Note**: It is not recommended to create a global alert because the alert can potentially be triggered by every group and monitor within SiteScope.

Alert Class	Description
Group Alerts	Alerts that are triggered when any monitor within the associated group or groups reports the category status defined for the alert. The following is an example of a group alert. Any monitor or subgroup within the group WebServers can trigger this alert.  New subgroups and monitors added within the associated group or groups after the alert definition is created are automatically associated with the alert.
Individual Monitor Alerts	Alerts that are triggered when any associated monitor reports the category status defined for the alert. The following is an example of an individual monitor alert. Only the associated monitor can trigger this alert.  Network SiteScope Network Interface SiteScope interface traffic Ping DHCP server New monitors added after the alert definition is created are not automatically associated with the alert but can be added by editing the alert definition.

You can create as many SiteScope alert definitions as you want. It is recommended however, that you plan and consolidate alerts to keep the number of alert definitions to a minimum. This facilitates alert administration and helps reduce redundant alert messages or actions.

Creating Alert Actions

When you create an alert scheme in SiteScope, you create alert actions to be triggered when the alert conditions are met. For a detailed list of available alert actions, see Types of Alert Actions.

You create alert actions using the Alert Action Wizard. While in the wizard, you determine the following:

- The type of alert action.
- The settings for the type of alert being sent. For example, you can define the recipients and their addresses for an e-mail alert action.
- The status condition that triggers the alert. For example, you can instruct SiteScope to trigger an alert action when a monitor's status changes to error or unavailable.
- The trigger settings that determine when the alert is triggered and when it is sent. For details, see "Understanding When SiteScope Alerts Are Sent" on page 1188.

You can create multiple alert actions for an alert scheme. For example, you can create an alert action to send a sound alert and another alert action to send an e-mail alert. Both are sent when the alert is triggered. You can also set different schedules for the different actions within the same alert definition. For example, you can schedule an e-mail alert action to be sent during regular working hours and an SMS alert action for evening and night hours. Both are triggered by the same change in condition but are sent at different times, depending on when the alert is triggered.

You can also make one alert action dependent on another alert action. This enables you to instruct SiteScope to send one type of alert when the trigger condition is first met and send another type of alert only when the first type of alert has been sent a number of times.

Creating alert actions for an alert enables you to copy those alert actions into other monitors or groups for use by other alerts. To use alert actions for other alerts, you must copy the alert and paste it into another monitor or group. All the alert actions for the alert are copied into the new alert. You can then edit the alert to be triggered for the new target monitor or group. For details, see "Copying and Pasting an Alert Definition" on page 1210.

For details on working with the Alert Action Wizard, see SiteScope Alert Actions - Action Type Page.

Understanding When SiteScope Alerts Are Sent

SiteScope triggers the alert as soon as any monitor it is associated with matches the alert trigger condition. The Trigger Settings options of the Alert Action Wizard allow you to control when alerts are actually sent in relation to when a given condition is detected. For example, you can choose to have SiteScope generate an alert only after an error condition persists for a specific interval corresponding to a given number of monitor runs. This is useful for monitors that run frequently that monitor dynamic, frequently changing environment parameters. In some cases, a single error condition may not warrant any intervention.

The options in the **Trigger Settings** are as follows:

When Option	Description
Escalate, after action <action name> occurred exactly N times	Only trigger an alert after another alert action has occurred the number of times defined in the text box. Use this option to create a dependency between alert actions defined for the same alert. **Example**: You want an e-mail alert sent only after an SMS alert defined for the same alert has been triggered three times. In this case, select the SMS alert action's name in the dropdown list of alert actions and 3 in the text box indicating the number of occurrences. **Note**: This option appears only if another alert action has been defined for the alert and if that alert action has the same trigger condition. For example, to trigger an alert on error.
Always, after the condition has occurred at least N times	Only trigger an alert after the condition occurs consecutively at least the number of times defined in the text box. This is a repeating alert. Once this condition is met, the alert is triggered each time the associated monitor is run until such time that the monitored system reports a change in status. Enter a value of **1** (one) to have the alert triggered for the first detected error or warning. Enter a number greater than one if you want to alert only on conditions that persist for more than a single scheduled monitor run.
Once, after condition occurs exactly N times	Only trigger an alert after the condition occurs consecutively for exactly the number of times indicated in the text box. Once this condition is met, the alert is triggered once. Enter a value of **1** (one) to have the alert triggered for the first detected error or warning. Enter a number greater than one if you want to alert only on conditions that persist for more than one scheduled monitor run.

When Option	Description
Initially alert X times, and repeat every Y times afterwards	Only trigger an alert after the condition occurs X consecutive times and then repeat the alert every Y consecutive times thereafter. This is a repeating alert. Once the Initial alert condition is met, the alert is triggered again after the associated monitor is run the number of times indicated in the second text box until such time that the monitored system reports a change in status. Enter a value of **1** (one) for the Initial alert value to have the alert triggered for the first detected error or warning.
Once, after X group errors	Cause an alert the first time that any monitor in the associated monitor group consecutively reports the trigger condition for the number of times indicated in the text box. This is a once-only group-wise alert. Once this condition is met, the alert is triggered once. Enter a value of **1** (one) to have the alert triggered for the first detected group error or warning. Enter a number greater than one if you want to alert only on conditions that persist for more than one scheduled monitor run.
Once, after all monitors in this group are in error	Only cause an alert when all of the monitors in the associated monitor group are in error. This is a once-only group-wise alert. Once this condition is met, the alert is triggered once. Use this alert for monitor groups used to watch redundant systems where a single failure may be acceptable, but multiple failures are not.
Only alert if monitor was previously in its selected status at least N times	Suppress the triggering of the alert until the subject monitor or group has reported the status selected (in warning or in error) for at least the number of times that you enter. Use this option to create an alert that signals that a server or service has become available again after it was offline or unavailable for an extended period.

The following diagrams show examples of different alert configurations that send alerts after the error condition has persisted for more than one monitor run. It is important to note that the sample interval corresponds to how often the monitor is run. If a monitor runs every fifteen seconds and the alert is set to be sent after the third error reading, the alert is sent 30 seconds after the error was detected. If the monitor run interval is once every hour with the same alert setup, the alert is not sent until 2 hours later.

Example 1a. An alert is sent for each time monitor is in error after condition persists for at least three monitor runs. Compare this with Example 1b below.

Alert setup	**Always, after the condition has occurred at least 3 times**								
sample interval	0	1	2	3	4	5	6	7	8
status	🟢	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🔴
count	c=0	c=1	c=2	c=3 alert!	c=4 alert!	c=5 alert!	c=0	c=1	c=2

Example 1b. An alert is sent for each time monitor is in error after condition persists for at least three monitor runs. Shows how the count is reset when the monitor returns one non-error reading between consecutive error readings. Compare this with Example 1a above.

Alert setup	**Always, after the condition has occurred at least 3 times**								
sample interval	0	1	2	3	4	5	6	7	8
status	🟢	🔴	🔴	🟢	🔴	🔴	🔴	🟡	🟢
count	c=0	c=1	c=2	c=0	c=1	c=2	c=3 alert!	c=0	c=0

Example 2. An alert is sent only once if monitor is in error for at least three monitor runs, regardless of how long the error is returned thereafter.

Alert setup	**Once, after the condition has occurred at least 3 times**								
sample interval	0	1	2	3	4	5	6	7	8
status	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
count	c=0	c=1	c=2	c=3 alert!	c=4	c=5	c=6	c=7	c=8

Example 3a. An alert is sent on the fifth time monitor is in error and for every third consecutive error reading thereafter. Compare this with Example 3b below.

Alert setup	**Initial alert 5 and repeat every 3 times afterwards.**								
sample interval	0	1	2	3	4	5	6	7	8
status	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
count	c=0	c=1	c=2	c=3	c=4	c=5 alert!	c=6	c=7	c=8 alert!

Example 3b. An alert is sent on the third time monitor is in error and for every fifth consecutive error reading thereafter. Compare this with Example 3a above.

Alert setup	**Initial alert 3 and repeat every 5 times afterwards.**								
sample interval	0	1	2	3	4	5	6	7	8
status	🟢	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴
count	c=0	c=1	c=2	c=3 alert!	c=4	c=5	c=6	c=7	c=8 alert!

Because you can create multiple alerts and associate more than one alert to a monitor, you can tell SiteScope to take more than one action for a given situation. For example, you can create one alert that tells SiteScope to page you whenever any monitor returns an error status. You can then create another alert that tells SiteScope to run a script file to delete files in the /tmp directory on your server if your Disk Space Monitor returns an error. If your disk becomes too full, SiteScope would page you because of the first alert definition and would run the script to delete files in the /tmp directory because of the second alert definition.

SiteScope alerts are generated when there is a change in state for a monitor reading. Thus you can set an alert for OK or warning conditions as well as error conditions. One way to take advantage of this is to add two alerts, one alert on error, and one alert on OK. Set alerts to be sent after the condition is detected 3 time. For the OK alert, check the box marked **Only allow alert if monitor was previously in error at least 3 times**. This prevents unmatched OK alerts, such as when a monitor was disabled for any reason (manually, by schedule, or by **depends on**) and then starts up again. This can also be used so that an OK alert is only sent after a corresponding error alert was sent. With these two alerts, you get a page when a link or service goes down (monitor detects change from OK to error), and another when it comes back up (monitor detecting change from error to OK). The following diagram is an example of using two alerts with a monitor.

Example 4. An Alert on error sent once for error after condition persists for at least three monitor runs. Alert on OK sent once for good status after at least one error or warning interval.

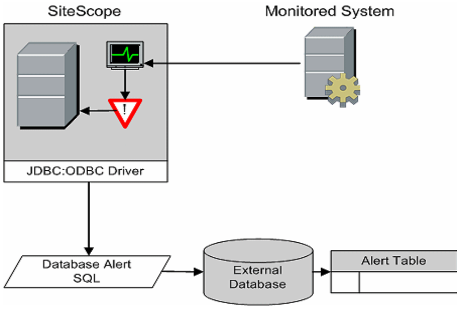
Alert on Error Setup	**On Error**		**Once, after the condition occurs exactly 3 times**						
Alert on OK Setup	**On OK**		**Once, after the condition occurs exactly 1 times** and **Only alert if monitor was previously in error at least 3 times**						
Sample Interval	0 🟢	1 🔴	2 🔴	3 🔴	4 🔴	5 🔴	6 🔴	7 🔴	8 🟢
Status									
Count	c=0	c=1	c=2	c=3 alert!	c=4	c=5	c=6	c=7	c=1 alert!

Once the monitor's status changes, the relevant status count is reset to zero.

Working with Database Alerts

You can use the Database Alert to forward system fault data and other status information to any SQL-compliant database.

The following diagram illustrates the Database Alert.



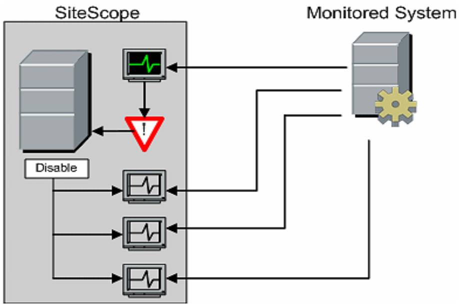
You need the following to be able to use the SiteScope Database Alert type:

- Access to an SQL compliant database.
- The applicable database connection URL which the SiteScope server uses to connect to the database.
- Installation of the applicable database middleware driver that the SiteScope application uses to communicate with the database on the SiteScope server.
- Database tables that have been created and structured to match the corresponding SQL statement that SiteScope uses to enter the alert into the database.

Working with Disable or Enable Monitor Alerts

The Enable/Disable alert type is useful for times when server maintenance or other activities are being performed that would logically result in errors for some monitors and cause unnecessary alerts to be generated.

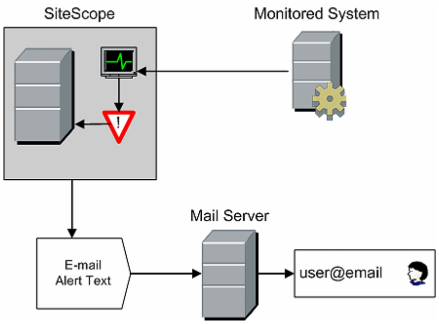
The following diagram illustrates an example of this alert type used to disable several monitors based on the condition reported to one monitor.



This alert type provides a functionality similar to the **Depends On** feature for building group dependencies between monitors and monitor groups. One important difference is that monitors disabled by this type of alert are not automatically re-enabled when the status of the subject monitor or group changes back to the original state. You can create one alert with an **Alert Category** of **Error** that disables monitors. You can then create a second alert with an **Alert Category** of **Good** that enables the same monitors.

Working with E-Mail Alerts

SiteScope E-mail Alerts send event notifications from SiteScope via e-mail as seen in the following diagram.



The SiteScope E-Mail Alert type requires:

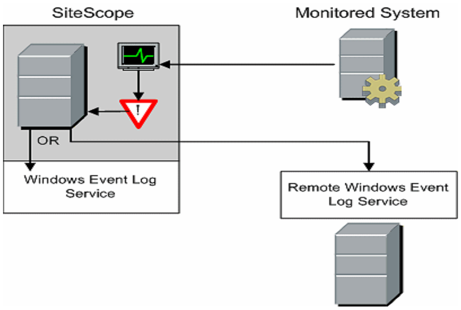
- Access to an active e-mail server
- One or more e-mail accounts that can receive the e-mail alerts
- SiteScope E-mail Preferences set to work with the external e-mail server

For more information on configuring SiteScope e-mail recipients, see “E-mail Preferences Overview” on page 207.

Working with Log Event Alerts

The Log Event Alert can be used to extend the types of events that are logged to a Windows Application Event Log. This provides a way to forward event data to log query systems that may not normally be logged by the Windows operating system.

The following diagram illustrates the Log Event Alert.



Use of the SiteScope Log Event Alert type requires:

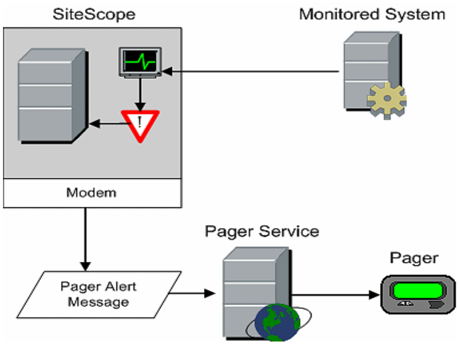
- Access to the Windows Event Log service. By default, this is the Event Log on the machine where SiteScope is running. The alert definition can be configured to send log events to another server.
- SiteScope running on a Microsoft Windows platform.

Important: If you are using SiteScope's Windows Event Log Monitor, you must use care when using the Log Event alert type because it is possible create an endless loop condition that can fill your Event log file. This can happen when a Windows Event Log Monitor detects an event that triggers a Log Event alert, which in turn puts an new event into the event log, which the Event Log Monitor then detects, and then triggers the Log Event alert, and so forth. To avoid this, Log Event alert types should not be associated with Windows Event Log Monitors.

Working with Pager Alerts

The Pager alert can be used to send event notification to electronic pagers. This is particularly useful when access to e-mail may not be available. Depending on the type of pager you use and the capabilities of the pager service, you can configure the Pager Alert to send a pager message with an abbreviated description of the problem or detected condition.

The following diagram illustrates the Pager Alert.



Use of the SiteScope Pager Alert type requires:

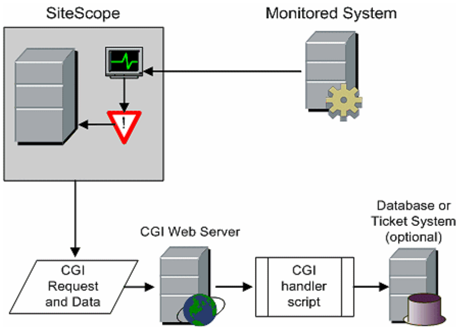
- Access to an active pager service
- A modem which the SiteScope server can use to connect to the pager service
- One or more pagers that can receive the pager alerts
- SiteScope Pager Preferences set to work with the modem and pager service

For more information on configuring SiteScope to use pager alerts, see “Pager Preferences Overview” on page 208.

Working with Post Alerts

The SiteScope Post alert uses the Common Gateway Interface protocol to forward POST data to a CGI enabled program. This can be used to forward event data to CGI script on another server that is a front-end for a trouble ticket system or reporting database. This alert type also provides a way of sending alert information through a firewall using HTTP or HTTPS without having to make other security changes.

The following diagram illustrates the Post Alert.



Use of the SiteScope Post alert requires:

- HTTP access between the SiteScope server and the server running the CGI script or server
- Format and syntax of the CGI POST request to the applicable CGI script or server

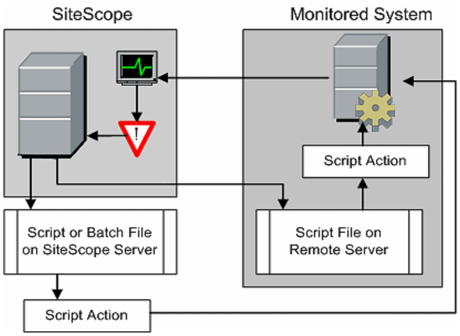
Working with Script Alerts

The most important components of Script Alerts are:

- The script definition itself.
- The monitor or monitors that are assigned to trigger the alert.
- The script to be executed by the alert.

The alert message template and resulting alert message file may also need to be considered depending what the script needs to do. You can use a script template, together with the **Parameters** setting to pass data to your script.

The following diagram illustrates the general concept of the script alert for both a local script and a script on a remote host.


SiteScope
Monitored System
Script Action
Script or Batch File on SiteScope Server
Script File on Remote Server
Script Action

The script alert definition or instance and the monitor or monitors that trigger the alert are handled as with other alerts or monitors in SiteScope. For example, you may create a monitor to watch a Web server running on a remote UNIX server. You can create a Script Alert associated with that monitor that executes a script to kill and restart the Web server process if the monitor reports an error.

Managing Script Files

Creating the script file to be called or executed by the Script Alert definition is another key step in using this automation capability in SiteScope. The specific commands and actions taken by the script are up to you. The script file should be written as a plain text file compatible with the operating system where the script is to be executed. This may be the same server where SiteScope is running or it may be on a remote machine to which SiteScope has access.

To run a script on the machine where SiteScope is running, the script file must be saved in the <**SiteScope install path**>/**SiteScope/scripts** directory on the SiteScope machine where the Script Alert is defined.

To run a script on a remote machine, you must save the script in a directory called **/scripts** in the home directory tree for the user account that SiteScope has execute permissions for on the remote machine.

The current execution directory when a script is run is <**SiteScope install path**>/**SiteScope/classes/** and not the **SiteScope/scripts/** directory. For commands executed by the script itself, the relative execution directory is <**SiteScope install path**>/**SiteScope/classes/**. Use full pathnames for any other file system commands or programs called by your script so that you do not need to worry about the current directory. Also, the server system environment variables may not have been set up for the script execution. This is another reason to use full pathnames for executables called by the script. If a script works when you run it from the command line but not from SiteScope, then you must determine what the error is.

Passing Data to a Script

SiteScope passes a number of parameters to the script as command line arguments. You can use this option to pass data to a script that can be used to modify a script's action. This adds versatility to the Script Alert.

By default, a SiteScope Script Alert passes seven command line arguments to a script. These are:

- The pathname of the scripts directory.
- The name of the monitor that caused the alert.
- The current status of the monitor.
- The pathname to the Alert Message File.
- The ID code of the monitor.
- The group the monitor is in.
- Any additional parameters specified on the **Parameters** text box in the alert form.

Two of these default arguments allows the script to access even more data. One is the Alert Message File and the other is the **Parameters** text box. The Alert Message File is a temporary text file created by SiteScope based on the alert template chosen for the Script Alert instance. Depending on the template you create or use, the Alert Message File may contain custom information as well as data specific to the monitor that triggered the alert. By passing the pathname to the Alert Message File to the script, you can have the script access this data.

You use the Parameters text box to specify individual monitor parameter data to be passed to the script. You can include multiple parameters by separating the parameters with spaces. This effectively allows you to increase the total number of parameters passed to the script. See the chapter on Template Properties in the SiteScope Reference Guide for more information on the parameters used for the different SiteScope monitors.

The pathname of the scripts directory can be useful in setting a execution path to another program as well as setting a directory path for any output written by the script.

For more information and examples of passing parameters and data to scripts, see "Writing Scripts for Script Alerts" on page 1311.

Troubleshooting Scripts

The scripts are run with the permissions of the account used by the SiteScope service. Some scripts may need extra permissions and you need to use the Services control panel to change the login account for SiteScope and then stop and start SiteScope. For example, scripts that restart services or reboot remote machines or scripts that copy protected files.

Since the script is run by the SiteScope service, anything done as part of your login may not have occurred in the script. For example, you can not rely on mapped drives, environment variables, or other login script items.

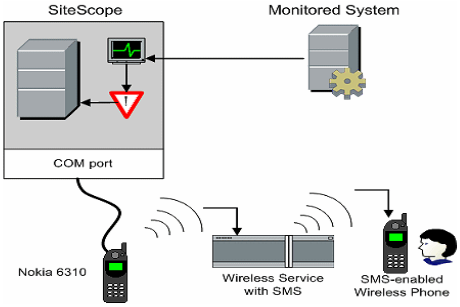
Since the script is run by the SiteScope service it can not receive any interactive input from a keyboard or other input device. Any script action or command that requires a user confirmation or input would cause the script to hang. Do not include any interactive commands requiring a user action as part of the script. Also, opening a WIN32 application (for example, Notepad) also causes the script to hang because it is waiting for the user to exit or close the application before continuing with the script execution.

Working with SMS Alerts

The SMS alert is an alternative to the Pager alert for communicating event notifications to mobile users without the use of e-mail. This alert type is current designed to transmit only the name of the SiteScope monitor that has reported an event condition and the status of that monitor as the content of the message.

Note: At present, the SMS alert can only be sent from SiteScope by using the hardware specified in this section. Consult the SiteScope Customer Support Knowledge Base for alternative ways of sending SMS messages using SiteScope.

The following diagram illustrates the SMS Alert.



The requirements for using the SMS alert include:

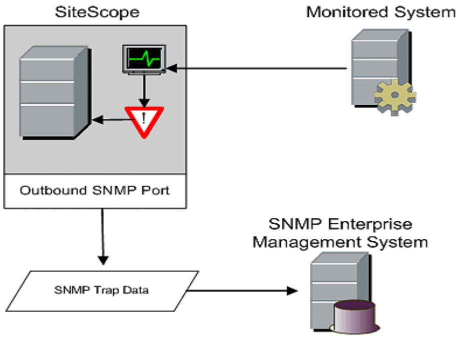
- An available serial communications port on the SiteScope machine that is sending the SMS alerts.
- A serial-to-wireless device interface cable, RS-232 Adapter Cable Nokia DLR-3P to connect the wireless transmitting device to the machine where SiteScope is running.
- An SMS-enabled wireless device connected to the SiteScope machine that is sending the alerts (that is, the Nokia 6310 phone using the interface cable).
- The necessary software to enable the SMS Alert (normally included with SiteScope 7.6c1 and later).

Note: Make sure that you do not have Nokia Data Suite, Palm Hot Sync, or any PDA software running on the server where SiteScope is running. These programs can bind the COM ports and prevent the dialer from working correctly.

Working with SNMP Trap Alerts

You can use the SiteScope SNMP Trap Alert to forward event data from any type of SiteScope monitor to an SNMP enabled host or management system. This means that SiteScope can be used to monitor and report events for applications and systems that do not have their own SNMP agent. For example, this can be used to send measurement data from a SiteScope Windows Performance Counter based monitor type or a URL monitor in the form of an SNMP trap.

The following diagram illustrates the SNMP Trap Alert.



Use of the SiteScope SNMP trap alert requires:

- Access to the applicable SNMP network ports
- SiteScope SNMP Preferences set to work with the applicable SNMP management console

For more information on configuring SiteScope to use SNMP alerts, see "SNMP Trap Preferences Overview" on page 209.

Working with Sound Alerts

It is important to note that the sound alert is limited to the machine on which SiteScope is running. Therefore, a sound alert is effective only if the SiteScope server is in an area that is regularly occupied by your support staff and the server is equipped with a sound card capable of processing the associated sound file.

Alternatively, SiteScope can be configured to embed an alert audio file into the Web pages served by SiteScope. This audio file is included with any SiteScope page that includes an error status for any monitor, such as the main panel or group detail pages. While this allows audio notification to all SiteScope clients through the user interface, it is not a true SiteScope alert and thus does not allow the same configuration options as the Sound Alert. For information on how to configure SiteScope to embed audio files for error notification, refer to the Knowledge Base http://support.mercury.com.

Manage Alert Definitions

Creating an Alert Definition

1. Select the SiteScope monitor group container or monitor element to which you want to associate the alert definition. Click the **Contents** tab on the right panel view menu and then click the **New Alert** button.

   Alternatively, right-click the container in the monitor tree and select **New Alert**. The Add Alert selection page is displayed in the content panel.

2. In the Main Settings pane, click **Add Action**. The Alert Action wizard begins. For details, see “SiteScope Alerts - Add/Edit Alert” on page 1211.

3. Complete the other panes. For details, see “SiteScope Alerts - Add/Edit Alert” on page 1211. Click **OK** to create the alert.

4 In the monitor tree, right-click the new alert and select **Test**. The Test Alert dialog box opens. From the drop-down menu, select a monitor instance to test and click **Test**. The Test Preferences dialog box opens with information about the alert test. If there were problems with the test, messages are displayed in the dialog box.

Note: The monitor you select does not have to be reporting the same status category that is selected to trigger the alert to test the alert. For example, the monitor does not have to currently be reporting an error to test an alert that is triggered by error conditions.

Editing an Alert Definition

Use any of the following methods:

- Select the alert and click the **Edit** button at the bottom of the Properties pane.
- Right-click the alert and select **Edit**.
- Select the container or element to which the alert definition is associated. Click the **Contents** tab in the right panel view menu. Click **Edit** to the right of the alert.

Customizing an Alert's Message Content

Note: Only alerts that have a template or that have message parameters can be customized. For more information on customizing alert templates, see "Customizing Alert Templates" on page 1317.

The following example shows how to change the SNMP Alert message from displaying the SNMP monitor's status to displaying a list of counters that are in Error state along with their values. This causes the message to only contain counters that breached the Error threshold and to omit all other counters.

Example

1 Edit the template file of the alert whose message content you want to change. In this example, the file is <SiteScope root dir>\templates.SNMP and contains the single line:
SiteScope\<group>\<name>\<sample>\<state>\

Replace the string <state> with the string <errorOnly>. The angle brackets (<,>) must remain around the text. The file now contains the single line:
SiteScope\<group>\<name>\<sample>\<errorOnly>\

Note: If you want to display a list of counters that are in Warning state, replace the string <state> with the string <warningOnly>.

2 Edit <**SiteScope root dir**>**groups****master.config** file and add the line
_errorOnlyDelimiter=,

with other similar error definitions.

In this example, the delimiter is a comma (,), but you can also use a space (" ") or a tab (\t). The added line in **master.config** looks something like:

```
_errorInsertHTML=
_errorOnlyDelimiter=,
_errorOnlyNewlineFormat=true
```

Note:

- If you used the string <**warningOnly**> in step 1, you must use the string **_warningOnlyDelimiter=<delimiter>** in **master.config**.
- If no **_errorOnlyDelimiter** is defined in **master.config**, the default delimiter is a space (" ").

Customizing Alert Template Tag Styles

The delimiter between items in the list can be changed if, for example, you have a parser that processes alert messages and needs a specific delimiter. You can also change the bracket delimiters that are used to identify variables. This is useful if you want the message read by XML and a variable replaced by an XML string.

To change the bracket delimiter:

1. Edit the template file for which you want to change the bracket delimiter. For example: <SiteScope root directory>/templates.mail/.
2. Use a text editor to add the following lines to the top of the relevant file:

   ```
   [Tag-Style:{}]
   ```

   Enter the characters after the colon (in this example {}) that should be used as the delimiter instead of the html brackets (<>).
3. Edit the relevant variables to be bracketed by the new characters defined in the Tag-Style string. For example: {state}.

Deleting an Alert Definition

Deleting an alert removes the applicable alert action from the SiteScope agent. It does not disable the associated monitors.

To delete an alert:

- ➤ Right-click the alert you want to delete and select **Delete**.
- ➤ Select the container or element to which the alert definition is associated. In the Alerts panel of the Contents pane, select the box of the alert you want to delete. Click to delete the alert.

Copying and Pasting an Alert Definition

You can copy an alert defined for a monitor or group into another monitor or group. The alert target automatically changes to the monitor or group into which the alert is copied.

Copying and pasting an alert definition is also useful for copied reusing existing alert actions that were created for an alert. When you copy/paste an alert definition, all the alert actions created for that alert are copied into the new alert. You can edit the alert settings for the new target of the alert and have all the alert actions as defined for the original alert.

Important: If you copy an alert definition from one group container to another, the **Alert Targets** for the pasted alert are automatically reset to include all of the children of the container into which the alert is pasted. After pasting an alert, edit the alert definition properties to be sure that the assigned **Alert Targets** are appropriate to the new alert context and your overall alerting plan.

To copy and paste an alert:

1. Right-click the alert definition you want to copy and select **Copy**.

   Alternatively, select the container or element to which the alert definition is associated. Click the **Contents** tab in the right panel view menu. Click the check box to the right of the alert and then click the **Copy** button.

2. Right-click the container or monitor element to which you want to add the copy of the alert definition and select **Paste** option from the action menu.

   Alternatively, in the **Contents** tab in the right panel view menu, click the **Paste** button.

3. Edit the pasted alert definition to verify the appropriate **Alert Targets** are selected.

68

SiteScope Alerts User Interface

This chapter includes the pages and dialog boxes that are part of SiteScope Alerts.

SiteScope Alerts - Add/Edit Alert

Description	Enables you to define alerts for a SiteScope, a group, or a monitor. **To access:** Right-click the SiteScope, group, or monitor for the alert. Select **New Alert**.
Important Information	Any field with a red asterisk (*) must be filled or the wizard does not proceed to the next step.
Useful Links	"Understanding Alerts" on page 1184

The following areas are found throughout the New Alert page:

Main Settings

The Main Settings section includes the following elements:

GUI Element	Description
Add Action	Deploys the Alert Action wizard to define an action to be done when an alert is triggered.
✎	Edits the alert action. This appears only after an alert action has been defined.
⧉	Duplicates the alert action. This appears only after an alert action has been defined.
✕	Deletes the alert action. This appears only after an alert action has been defined.
Alert Actions	The columns in this table are defined in the Alert Action wizard: ➤ **Name.** The name given to the alert action in the SiteScope Alert Actions - Action Type Page. ➤ **Category.** The category selected in the Trigger Page that triggers the alert action. ➤ **When.** The schedule selected in the Trigger Settings Page for when the alerts are sent. ➤ **Schedule.** The daily/weekly schedule selected in the Action Type Settings Page. For a complete description of each action type, see "Types of Alert Actions" on page 1235.

GUI Element	Description
Alert Name	Enter a text description for this alert definition. This name is used to identify this alert definition in the product display.
Alert Targets	Use the context menu tree to the right of this item to select the groups and/or monitors to trigger this alert. The context menu includes the currently selected object and all of the child objects. Check the box beside the current object to associate this alert with all objects within this object. Check one or more individual object to associate this alert definition to the selected objects. Alternatively, you may select the SiteScope root and then define an alert filter rule in the Filters Settings to limit alerting to those objects that match the conditions set in the filter.

Enable/Disable Alert

The Enable/Disable Alert section includes the following elements (listed alphabetically):

GUI Element	Description
Disable Description	(Optional) Description of the purpose of the disable operation.
Disable This Alert	Use to manually control the generation of alerts. This can be useful when the systems being monitored are off-line for maintenance or if the recipient of the alerts is unavailable for a period of time. ➤ **Enable Alert.** Overrides any disable action on the alert and enables the alert for execution based on the conditions defined. ➤ **Disable Alert Indefinitely.** Prevents SiteScope from executing the alert action even if the alert condition is met until this radio button is cleared and the alert definition is updated. **Note:** Use of this option may result in loss of expected alert capability if the alert is disabled to accommodate a temporary condition. It is important to review this status later to manually enable the alert definition, as needed. ➤ **Disable Alerts for the Next Time Period.** Prevents the execution of the alert action for the time period you enter, even if the alert condition is met. The alerts are disabled immediately and re-enabled when the time period expires. **Default Value:** 10 minutes. ➤ **Disable on a One-Time Schedule from Time1 to Time2.** Prevents SiteScope from executing the alert action for the time period indicated, even if the conditions are met. The alerts are disabled at the beginning of the time period and re-enabled after the time period expires.

Filter Settings

Description	Creates filter conditions to limit the alert action to only those monitors that match the criteria you entered. You can define alerts for a large number of monitors and then apply a filter so that only certain monitors within the selected list actually trigger the alert. This can simplify the creation of alert definitions and alert management. **To access:** Right-click the SiteScope, group, or monitor for the alert. Select **New Alert**.
Important Information	To disable alert filtering, clear the applicable fields and update the alert definition.

The Filter Settings section includes the following elements (listed alphabetically):

GUI Element	Description
Monitor Type Match	Limits the alert action to a monitor type from the set of monitors associated with this alert. You choose multiple types.
Name Match	Suppresses the alert for all associated groups or monitors except those with a specific text appearing as part of their name. ➤ Enter a regular expression in this text box to match a name string pattern. For details, see “Using Regular Expressions in SiteScope” on page 1282. ➤ Enter all or part of the monitor name string you want to use as a filter criteria. For example, entering the string URL: limits this alert to monitors whose name contains the string URL:. **Note:** The match is case sensitive.

GUI Element	Description
Status Match	Suppresses the alert for all associated monitors except those returning a specific status text. ➤ Enter a string that you expect to appear in the status text for the monitor you want to trigger this alert. For example, if you enter the text timeout in this box, an alert is only triggered by a monitor associated with this alert that also has a status of timeout. ➤ Enter a regular expression in this text box to match a status string pattern. For details, see "Using Regular Expressions in SiteScope" on page 1282. **Note:** The match is case sensitive.

Category Settings

The Category Settings section includes the following elements:

GUI Element	Description
Assigned Categories	For details, see "Working with Categories" on page 173.

Advanced Settings

The Advanced Settings section includes the following elements:

GUI Element	Description
Description	You can enter free text to give a description to this alert. This description does not appear in any other context. It appears only when editing the alert.

SiteScope Alert Actions - Action Type Page

Description	The first page in the Alert Action wizard. Use the Alert Action wizard to configure actions to be taken when an alert is triggered. **To access:** In the Main Settings section of the Add Alert page, click **Add Action**. Use the Action Type Page to define the SiteScope Alert name and type.
Important Information	You can only select one type of alert at a time. If you are editing an alert, you cannot change the action type, the action to be done when an alert is triggered. For example, if an alert's action type was E-mail, you cannot change it to SMS. You must delete the alert and create an alert whose action type is SMS.
Wizard Map	The Alert wizard includes: **SiteScope Alert Actions - Action Type Page** > Action Type Settings Page > Trigger Page > Trigger Settings Page.

The page includes the following elements (listed alphabetically):

GUI Element	Description
Action Name	The name given to the action to be done when the alert is triggered. It is not the name of the alert. For example, if you want to configure an alert to check the CPU of all Solaris machines and send an SMS message when some alert is triggered, you could define the alert name in Main Settings to be Solaris_CPU and the action name to be send_sms.
Database	Sends an alert message with a description of the problem as a record to a SQL database. You can then use database tools to provide more advanced recording, sorting, and reporting on your monitoring data.

GUI Element	Description
Disable or Enable Monitors	Automatically enables or disables monitors or monitor groups based on a change of state in another monitor.
E-Mail	Sends an e-mail message to one or more e-mail addresses with a description of condition that triggered the alert.
Log Event	Logs events to the Windows Application Event Log. Entries in the event log can then be viewed with the Event Viewer and/or used by other software utilities that perform centralized alerting from the event log.
Pager	Sends a message to a pager to signal that SiteScope has detected a particular condition.
Post	Submits a CGI POST message to a CGI script, servlet, or other CGI-enabled program. The message contains a description of a monitor condition .
Script	SiteScope can execute scripts or batch files when the alert condition is met. The script or batch file can execute a system command or a program in any language that can be called from a command line entry. You can use this alert to execute recovery scripts that automatically respond to critical conditions or failures (for example, to reboot a server or to copy files).
SMS	Sends a short text message using the Short Message Service (SMS) to an SMS-enabled mobile phone or wireless device.
SNMP Trap	Sends an SNMP trap to an SNMP management console or host. This enables SNMP reporting of system parameters not normally supported by SNMP agents.
Sound	Plays a sound or audio file on the machine on which SiteScope is running when an event has been detected

Action Type Settings Page

Description	Use the Action Type Settings page to define the settings that are specific to the alert type.
Important Information	The settings vary according to the type of alert action you selected in the SiteScope Alert Actions - Action Type Page.
Wizard Map	The Alert Action wizard includes: SiteScope Alert Actions - Action Type Page > **Action Type Settings Page** > Trigger Page > Trigger Settings Page.

Database Alert Properties

The following properties must be entered for the **database** alert (listed alphabetically):

GUI Element	Description
Backup Database Connection URL	If a backup database for SiteScope alert logging is required, this is the URL to the backup database connection to use if the main database connection fails. **Example**: If the ODBC connection for the backup database connection is called testdb2, the URL would be jdbc:odbc:testdb2.

GUI Element	Description
Database Connection URL	The URL to a database connection. **Example**: In Windows NT, use the ODBC Data Sources manager in the Settings control panel to create a connection called test and then enter jdbc:odbc:test as the database connection URL. **Note for using Windows Authentication:** If you want to access the database using Windows authentication, enter jdbc:mercury:sqlserver://<server name or IP address>:1433;DatabaseName=<database name>; AuthenticationMethod=type2 as the connection URL, and com.mercury.jdbc.sqlserver.SQLServerDriver as your database driver. Leave the **Database User name** and **Database Password** boxes empty, since the Windows user credentials of the account from which the SiteScope service is running are used to establish a connection to the database.
Database Driver	The Java class name of the JDBC database driver. SiteScope uses the same database driver for both primary and backup database connections. If a custom driver is used, the driver must also be installed in the SiteScope/java directory. See “Database Query Monitor Overview” on page 469 for more information about setting up database drivers for SiteScope. **Default Value:** sun.jdbc.odbc.JdbcOdbcDriver
Database Password	The password to connect to the database.
Database User Name	The user name to connect to the database.
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. **Default Value:** every day, all day

GUI Element	Description
SQL Statement	The SQL statement used to add the alert to the database. Items enclosed in angle brackets (< and >) are replaced with fields from the monitor that triggered the alert. **Default Value:** INSERT INTO SiteScopeAlert VALUES('<time>', '<group>', '<name>', '<state>')

Disable/Enable Monitors Alert Properties

The following properties must be entered for the **disable/enable monitors** alert (listed alphabetically):

GUI Element	Description
Group/Monitors Action	You can choose whether this alert action disables a monitor or enables a monitor when the alert is triggered. **Default Value:** Disable
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. **Default Value:** every day, all day
Targets	The groups and monitors that should be affected by the action of this alert. The list includes all groups and monitors configured for the SiteScope. You can select any group or any monitor running in any group for this alert action. Press CTRL RIGHT to select multiple items. **Example:** This alert action is being configured for a Disk Space monitor. An alert triggered for this monitor can disable all CPU monitors monitoring the same server.

E-Mail Alert Properties

The following properties must be entered for the **e-mail** alert (listed alphabetically):

GUI Element	Description
Addresses	Separate multiple e-mail addresses with a comma (,). The addresses are checked for valid syntax but not for other errors (for example, that the e-mail user exists).
Mark This Action to Close Alert	When the status changes and the alert trigger condition is no longer true, this action closes the alert and sends a close notification by adding the word **Close** to the message sent. **Default Value:** The check box is cleared.
Recipients	Enter e-mail recipients who have been configured in Mail Preferences. For details, see "E-mail Preferences Overview" on page 207.
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. You cannot edit this value. It is determined by the schedule defined for the mail recipients in preferences.
Template	A drop-down list of all templates for the e-mail alert action. In an E-mail alert action, select the **ShortMail** template for a shorter e-mail message. Other options allow you to choose the level of detail to include in E-mail alerts. **Default Value: Typical** template includes the following values: Monitor: <groupID>:<name>; Group: <group>; Status: <state>; Sample #: <sample>; Time: <time> **Note**: You can add additional templates into the **<SiteScope install path>/SiteScope/templates.mail** directory. For details on the available templates, you can open the files in this directory in a text editor to see what values are sent with each option.

Log Event Alert Properties

The following properties must be entered for the **log event** alert (listed alphabetically):

GUI Element	Description
Category ID	Used as the <category ID> for the event created by this alert. **Default Value:** 0
Event ID	A number used to set the <ID> field of the event that is logged. **Syntax:** must be numeric. **Default Value:** 1000
Event Source	A string used to set the <Source> field of the logged event. **Syntax:** must be text. **Default Value:** SiteScope
Event Type	**Default Value:** the monitor status. In other words, the Event Type is Error for an Error status, Warning for Warning, and Informational for monitors reporting a status of Good.
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. **Default Value:** every day, all day

GUI Element	Description
Send To	The name of the Windows machine where the event is to be appended to the event log. **Default Value:** localhost (the machine where SiteScope is running).
Template	A drop-down list of all templates for the log event type alert action. **Default:** Default template **Note**: You can view the contents of the existing templates or add additional templates in the **<SiteScope install path>/SiteScope/templates.eventlog** directory.

Pager Alert Properties

The following properties must be entered for the **pager** alert (listed alphabetically):

GUI Element	Description
Mark This Action to Close Alert	When the status changes and the alert trigger condition is no longer true, this action closes the alert and sends a close notification by adding the word **Close** to the message sent. **Default Value:** the check box is cleared.
Message	The content is determined by the type of alert you are defining: For Pager Alerts, the maximum length is 32 characters.
Pager Recipients	Enter pager recipients that have been configured in Pager Preferences. For details, see "Pager Preferences Overview" on page 208.

GUI Element	Description
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. You cannot edit this value. There is a predefined schedule for pager recipients defined in preferences.
Template	A drop-down list of all templates for the pager alert action type. **Default:** Default template **Note**: You can view the contents of the existing templates or add additional templates in the **<SiteScope install path>/SiteScope/templates.page** directory.

Post Alert Properties

The following properties must be entered for the **post** alert (listed alphabetically):

GUI Element	Description
Authorization Password	This is the password for the Authorization User Name in a Post Alert. Alternatively, leave this entry blank and enter the password in the Default Authentication Credentials section on the General Preferences page. Use this method to define common authentication credentials for use with multiple monitors.
Authorization User Name	This user name permits access to the URL of the CGI script in a Post Alert. Not all CGI scripts require a user name. Alternatively, leave this entry blank and enter the user name in the Default Authentication Credentials section in the General Preferences page. Use this method to define common authentication credentials for use with multiple monitors.

GUI Element	Description
HTTP Proxy	The domain name and port of an HTTP Proxy Server used to access the URL of the CGI script.
Post to URL Form	The URL of the CGI script that SiteScope should submit to the alert. For example, http://admindb.server.net/cgi-bin/error.pl. **Syntax:** You must include the string **http:**//. There is syntax checking for a valid URL address.
Proxy Server Password	The user name and password to access the URL of the CGI script, if required by the proxy server. Your proxy server must support Proxy-Authenticate.
Proxy Server User Name	
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. **Default Value:** every day, all day
Template	A drop-down list of all templates for the post alert action type. **Default:** Default template **Note**: You can view the contents of the existing templates or add additional templates in the **<SiteScope install path>/SiteScope/templates.post** directory.

Script Alert Properties

The following properties must be entered for the **script** alert (listed alphabetically):

GUI Element	Description
Parameters	Additional monitor parameters that you can pass to your script, such as: ➤ path name of the scripts directory ➤ name of the monitor that caused the alert ➤ current status of the monitor ➤ path name to the alert message file ➤ ID of the monitor ➤ monitor group These parameters are sent as the seventh, eighth, ninth, and so forth, command line arguments respectively. The parameters available to be passed to the script are dependent on the type of monitor that triggers the alert. **Syntax:** Surround the property name variable in the properties list with angle brackets (< >). For example, to pass the server name to the script, enter <_machine> in the text box. To pass more than one extra parameter, separate the parameters with a single space. This is the same way the arguments would be added on the command line. **Default Values:** The Script Alert always passes the above parameters to a script as command line arguments. They do not need to be listed here.
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. **Default Value:** every day, all day

GUI Element	Description
Script	The script to run in response to the selected condition. You can create as many custom scripts as you need. Place them in <**SiteScope install path**>/**SiteScope/scripts** directory or the applicable scripts directory on a remote machine. SiteScope lists all files found in this directory on the selected server in the drop-down list.
Server	The server on which the script should be run. The scripts directory must be in the directory tree of the remote login account that allows remote scripts to be invoked by SiteScope.
Template	A drop-down list of all templates for the script alert action type. **Default:** Default template **Note**: You can view the contents of the existing templates or add additional templates in the <**SiteScope install path**>/**SiteScope/templates.script** directory.

SMS Alert Properties

The following properties must be entered for the **SMS** alert (listed alphabetically):

GUI Element	Description
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. **Default Value:** every day, all day
SMS Number	The telephone number required by the SMS service that identifies the destination for the message. **Syntax:** Numeric only. Maximum of 9 digits.

SNMP Trap Alert Properties

The following properties must be entered for the **SNMP trap** alert (listed alphabetically):

GUI Element	Description
Mark This Action to Close Alert	When the status changes and the alert trigger condition is no longer true, this action closes the alert and sends a close notification by adding the word **Close** to the message sent. **Default Value:** the check box is cleared.
Message	The content is determined by the type of alert you are defining: ➤ **SNMP Trap Alert.** The prefix to be added to the SNMP trap sent by this alert.
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. **Default Value:** every day, all day
SNMP Trap	The SNMP Trap to trigger an alert. **Default Value:** Default

GUI Element	Description
Template	A drop-down list of all templates for the SNMP trap alert action type. Each line in the template is sent as a separate SNMP variable. The template file can also be modified using: ➤ [Agent Host: <hostname-or-ip-address>] as the first line of the template, to send the trap with that hostname or IP address as the source of the trap. By default, the IP address of the machine that SiteScope is running on is used as the source of the trap. ➤ [Command: <command name>] to override the default command. ➤ [Type: <var-type>] to override the default type of the object. [OID: <object id>] to change the default object id. For example, use this to change a var-binding variable object id. **Default:** Default template **Note**: You can view the contents of the existing templates or add additional templates in the <**SiteScope install path**>/**SiteScope/templates.snmp** directory.

Sound Alert Properties

The following properties must be entered for the **sound** alert (listed alphabetically):

GUI Element	Description
Schedule	The daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. **Default Value:** every day, all day
Sound File	Additional sounds can be added to the <**SiteScope install path**>/**SiteScope/templates.sound** directory in AU format (8 bit, &#micro;law, 8000 Hz, one-channel) with an .au suffix.

Trigger Page

Description	Use the Trigger page to select the status of the object type that triggers an alert action.
Wizard Map	The Alert wizard includes: SiteScope Alert Actions - Action Type Page > Action Type Settings Page > **Trigger Page** > Trigger Settings Page.

The page includes the following elements (listed alphabetically):

GUI Element	Description
Alert Category	Alerts are triggered when the status changes from one state to another. Select the category that triggers the alert action. The categories are: ➤ **Error.** Alerts are triggered if the monitor was previously reporting a status of Good. ➤ **Good.** Alerts are triggered if the monitor was previously reporting a status of Error. ➤ **Unavailable**. Alerts are triggered if the monitored machine was previously available and is no longer. ➤ **Warning.** Alerts are triggered if the monitor was previously reporting a status of Good. **Default Value:** Error

Trigger Settings Page

Description	Use the Trigger Settings page to select the trigger frequency.
Important Information	The available options vary according to what you chose in the Trigger Page. For more detailed information on the options here, see “Understanding When SiteScope Alerts Are Sent” on page 1188. **Warning:** When editing an alert within the Alert Action Wizard, the trigger settings may reset to their default selections if you click **Back** and then **Next** to return to the Trigger Settings page.
Wizard Map	The Alert wizard includes: SiteScope Alert Actions - Action Type Page > Action Type Settings Page > Trigger Page > **Trigger Settings Page**.

The page includes the following elements:

GUI Element	Description
Escalate, after action <> occurred exactly N times.	Select this option if the alert action you are creating is dependent on another alert action. You must select the name of the alert action on which this alert action is dependent and the number of times the first alert action is triggered before this alert action is triggered. **Example**: You created an alert action to send a sound alert when a certain condition is met. You want an E-mail alert to be sent when the sound alert action has been triggered 3 times. Select the name of the sound alert action and 3. **Note**: This option appear only if another alert action has been defined for the alert.
Always, after the condition has occurred at least N times.	After the alert conditions have occurred at least N times, the alert is triggered every time the alert conditions are met again after the initial trigger. Enter the minimum number of times the alert condition must be met before the alert is triggered the first time. **Default Value:** Once, after condition has occurred exactly 1 time **Syntax:** numeric only **Range:** 1-99
Once, after condition occurs exactly N times.	The alert is triggered only once after the alert condition is met for the Nth time. Enter the number of times the alert conditions must be met before the alert is triggered. **Syntax:** numeric only **Range:** 1-99

GUI Element	Description
Initially after X times, and repeat every Y times afterwards.	The alert is triggered after the alert condition occurs X consecutive times, and then the alert is triggered every consecutive Y occurrences that the alert conditions are met. For example, if X is set to 3, and Y is set to 4, then the alert action would be done on the 3rd, 7th, 11th, and so forth, occurrences of the alert condition. **Syntax:** numeric only **Range:** 1-99
Once, after N group errors.	This is displayed if you chose **Error** in the Trigger Page. The alert is triggered only after any monitor in the group has reported the alert condition exactly N consecutive times. **Note:** This option is only available for SiteScope groups.
Once, after all monitors in this group are in error.	This is displayed if you chose **Error** in the Trigger Page. The alert is triggered the first time all monitors in the group are in error. **Note:** This option is only available for SiteScope groups.
Only alert if monitor was previously in error/warning	This is displayed if you chose **Good** or **Warning** in the Trigger Page. This option suppresses the triggering of the alert until the subject monitor or group has reported a status of either of the following: ➤ **Error** or **Warning** for alert category **Good** ➤ **Good** or **Error** for alert category **Warning**, for at least the number of times that you entered

Types of Alert Actions

GUI Element	Alert Action Name	Description
🛢	Database	Sends an alert message with a description of the problem as a record to a SQL database.
✉	E-mail	Sends an e-mail message to one or more e-mail addresses with a description of the error or warning.
🖥	Enable/Disable	Manually controls the generation of alerts.
📝	Log	Logs events to the Windows Application Event Log.
📟	Pager	Sends a message to a pager to signal that SiteScope has detected a particular condition.
HTML	Post	Submits a CGI POST containing a description of a monitor condition to a CGI script, servlet, or other CGI-enabled program.
📜	Script	SiteScope can execute scripts or batch files when the alert trigger condition is detected. The script or batch file that is called can execute a system command or a program in any language that can be called from a command line entry.
📱	SMS	Sends a short text message using the Short Message Service (SMS) to an SMS-enabled mobile phone or wireless device.
▦	SNMP Trap	Sends an SNMP trap to an SNMP host or management console.
🔈	Sound	Plays a sound or audio file on the machine on which SiteScope is running when an event has been detected

69

Introducing SiteScope Reports

Knowing the current status of parameters that SiteScope is monitoring is only half the battle. It is also important to know how the servers and applications you are monitoring have performed over time and to review the monitoring environment. SiteScope reports are important tools in monitoring and troubleshooting operational performance and availability.

You can generate a report for a single monitor, several monitors, or even several monitor groups. Report definitions include several report content options including tables of specific monitor measurements, summaries of results, and graphs.

SiteScope reports can be valuable to many people in your organization, including management personnel in Sales, Marketing, Customer Support, and Operations. SiteScope User accounts can be created to allow these users restricted access to the SiteScope service to view reports. See the section "User Preferences Overview" for more information.

Note: To view certain report elements on SiteScope for UNIX/Linux, it is necessary that an X Window system be running on the server where SiteScope is running.

SiteScope include four kinds of management reports. The following describes the report types and their usage.

- **Alert Reports.** This report is an ad hoc or custom report used to display SiteScope alerts sent over specific time periods. Alert reports do not support exporting data. The settings for an Alert report are not saved to the SiteScope configuration data for later use. See Chapter 70, "Alert Report" for more information.
- **Management Reports.** Reports that are generated automatically based on the schedule option you choose. When the schedule interval is met, SiteScope reads the applicable log files and generates the report based on the applicable monitor measurement information for the time interval specified. The report data can be saved to a file format suitable for importing into a spreadsheet or other application. See Chapter 71, "SiteScope Management Reports" for more information.
- **Quick Reports.** This report is an ad hoc or custom report used to look at specific time periods and monitors as needed to look at particular events or problems. Quick reports do not support exporting data. The settings for a Quick report are not saved to the SiteScope configuration data for later use. See Chapter 72, "SiteScope Quick Report" for more information.
- **Monitor Summary Reports.** This report is an ad hoc report you use to review configuration properties and settings for existing monitors. Monitor Summary reports can be exported in one of three text data formats. The settings for a Monitor Summary report are not saved to the SiteScope configuration data for later use. See Chapter 73, "Monitor Summary Report" for more information.

SiteScope monitor data available for generating reports is limited to the amount of log data stored on the SiteScope server. By default, SiteScope retains monitor data log files for 40 days. The log files are rotated and files older than the log retention period are automatically deleted.

Note: Keeping monitor data logs for longer periods can cause a data storage problem for the SiteScope server depending on the total number of monitors configured and how often the monitors run per day. You should monitor the size of log files in the **SiteScope\logs** directory to estimate the data accumulation rate.

You can change the length of time that SiteScope retains monitor data using the log preferences. You can configure SiteScope to export monitor data to an external SQL-compliant database to maintain monitor data for longer periods or to make the data available to other reporting applications. For details, see “Log Preferences Overview” on page 204.

70

Alert Report

The Alert Report provides you with information about SiteScope alerts generated during a specified time period.

Working with Alert Reports

You use SiteScope Alert Reports to view alerts data for any time period that you select. Alert reports are generated only on demand rather than automatically at regular intervals as with SiteScope Management Reports.

When you choose to generate an Alert Report, SiteScope reads the applicable log files and generates the report based on the applicable alert triggering information and the time interval you specify.

Alert Reports are ad hoc reports and their definitions are not stored for future use. No report element is added to the monitoring tree for this report type.

Generating an Alert Report

Use the following steps to generate an Alert Report.

To generate a report:

1 On the left navigation tree, select the monitor group container or monitor element that encompasses all of the monitor and group elements you want to include in the Alert Report.

2 Right-click the container or monitor element to display the container action menu and select **New report**. The report selection page is displayed in the content panel. Alternatively, you can click the **Contents** tab from the right panel view menu, and click the **New Report** button at the top of the Contents view.

3 Select the **Alert** link. The New SiteScope Report page is displayed.

4 Complete the items in the **Main Settings** as described in the section below.

5 When the required settings are defined, click the **Apply** button to create the report. The report output is displayed in a new browser window.

Configuring Alert Report Settings

An Alert Report can be generated for any SiteScope monitor group container or individual monitor in the monitor tree. You configure the report using the Main Settings section to select which alert types to include in the report, the time period of the report, and the detail level.

Alert types

Choose the alert types that you want to include in the report. By default, all alert types are included in the report. Use the CTRL and SHIFT keys to select more than one alert type.

Alert time period

Specify the period of time that you want the Alert Report to cover. Enter the time from which you want the report coverage to start in the **From** boxes and the time to which you want to cover in the **To** boxes. Note that times should be entered in 24-hour format. By default, the alert time period is from one hour before the time that the Alert Report is generated until the current time. Click **Apply** to validate the time period.

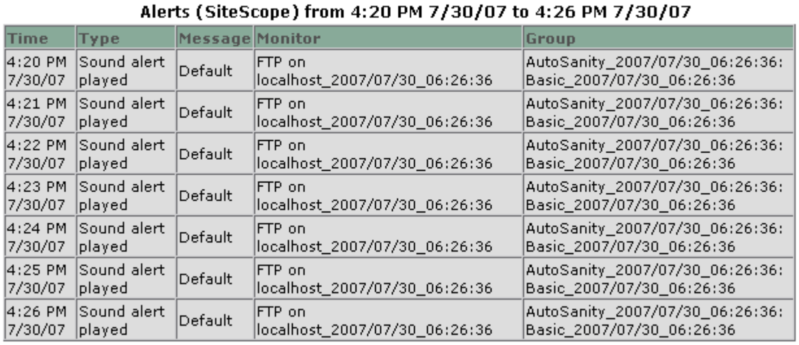
Detail level

Select the level of detail to include in the Alert Report. The options for the Alert detail level are:

- **Basic.** Displays the time and summary information for each alert sent. This is the default setting.
- **Show Detail for Failed Alerts.** Displays the time and summary information for each alert, and a full diagnostics breakdown for each failed alert.
- **Show Detail for All Alerts.** Displays detailed alert information for each alert in the report.

Reading the Alerts Report

The Alerts Report is presented in a table format. Data in the report include information about the configuration and current settings of monitors in the groups you have selected to include in the report. Below is an example of an alert report.



Alerts (SiteScope) from 4:20 PM 7/30/07 to 4:26 PM 7/30/07

Time	Type	Message	Monitor	Group
4:20 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:21 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:22 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:23 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:24 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:25 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36
4:26 PM 7/30/07	Sound alert played	Default	FTP on localhost_2007/07/30_06:26:36	AutoSanity_2007/07/30_06:26:36: Basic_2007/07/30_06:26:36

The report includes the following:

- The name of the monitor group container or individual monitor for which the report was created. This is located in the report title.
- The time period that the report covers. This is located in the report title.
- The time an alert was triggered, the alert type, and the alert message. This is located in the report table.
- The name of the monitor and group on which the alert was triggered. This is located in the report table.

71

SiteScope Management Reports

You use the Management Report definition form to define the monitor parameters you wish to measure. You choose a schedule option to determine when to generate the report.

Introducing Management Reports

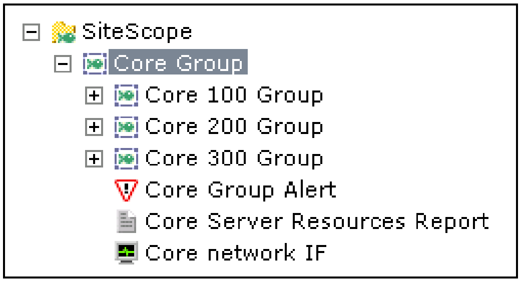
Management Reports are designed to provide you a summary of system availability data for a given time period. Management reports are generated directly from data collected by your SiteScope monitors. Reports give you a summary and specific details of system availability and performance. You can also use them to detect emerging trends and correct potential problems before they become a crisis.

SiteScope Management reports are generated automatically by SiteScope at an interval that you specify and are stored on the SiteScope server. You use the View Report tab to access these reports. See the section “Understanding the View Report Tab” on page 1251 for more information.

By default, SiteScope keeps the 10 most recently generated reports. This means that hourly reports are available for the last 10 hours, daily reports are available for 10 days, weekly reports are available for 10 weeks, and so forth. You can change this report storage period by changing the value of the _maximumReports setting in the SiteScope **master.config** file.

Working with SiteScope Management Reports

Reports are added as elements to the SiteScope menu tree. They can be added as a child to the SiteScope node, to a monitor group, or to an individual monitor. The following figure is an example of how reports are displayed in the left menu tree.



Reports have a scope based on the container to which they are added. You add a report to the container or element that contains all of the monitors whose data you want to include in the report. You then use the **Monitors and Groups to report on** setting in the Report Properties tab to narrow the selection of monitors to be included in the report.

You can create as many SiteScope report definitions as you want. It is recommended however that you plan and consolidate reports to keep number of report definitions to a minimum. This can facilitate report administration and help reduce redundant report messages or actions. When creating a report for a large number of monitors, you should consider making separate reports based on the type of monitor or measurement. For example, when reporting on system resources for 20 different remote servers, consider making one report with monitors that measure numeric values such as CPU or disk space and another report for monitors that report basic availability such as services or processes.

Creating a Management Report Definition

Use the following steps to create a report definition.

To create a new report definition:

1 Using the left menu, select the SiteScope monitor group container or monitor element to which you want to associate the report definition.

2 If necessary, click the **Contents** tab from the right panel view menu. The applicable Contents panel is displayed.

3 Click the **New Report** button at the top of the Contents view or at the bottom of the reports section of the Contents area. Alternately, you can right-click the container in the left menu to display the container action menu and select **New report**. The report selection page is displayed in the content panel.

4 Select the **Management** link. The New SiteScope Report page is displayed.

5 Complete the items in the **Main Settings** as described in the section below. If necessary, complete the items in the **Advanced Settings** and other sections as described in the sections below.

6 When the required settings are defined, click the **Add** button to create the report definition.

Editing a Management Report Definition

You may edit a report at any time. The two main methods to edit a report are as follows:

To edit a report definition using the left menu:

1 Using the left menu, select the report definition element you want to edit.

2 Select the Properties tab in the right hand content area and click the **Edit** button at the bottom of the properties panel. Alternately, you can right-click the report object in the left menu to display the report action menu and select **Edit**.

3 Make the desired changes to report definition in the report properties panel.

4 Click the **OK** button to save the changes.

To edit a report definition using the container Contents panel:

1. Using the left menu, select the container or element to which the report definition is associated.
2. If necessary, click the **Contents** tab from the right panel view menu. The applicable Contents panel is displayed.
3. In the reports section of the Contents panel, click the **Edit** icon button to the right of Description column for the applicable report definition. The applicable report properties panel is displayed.
4. Make the desired changes to report definition in the applicable report properties panel.
5. Click the **OK** button to save the changes.

Deleting a Management Report Definition

Deleting a Management report definition discontinues the generation of applicable report. Previously generated reports continue to be available until the underlying data is removed. As with other actions, there is more than one method that can be used to delete a report definition.

To delete a report definition using the left menu:

1. Using the left menu, select the report definition element you want to delete.
2. Right-click the container in the left menu to display the container action menu and select **Delete**. A confirmation message is displayed.
3. Click **OK** to confirm the action. The report definition is deleted.

To delete a report definition using the container Contents panel:

1. Using the left menu, select the container or element to which the report definition is associated. The applicable Contents panel is displayed.
2. In the reports section of the Contents panel, check the box corresponding to the report definition you want to delete.
3. Click the **X** button at the bottom of the reports section to delete the selected report definitions. A confirmation message is displayed.
4. Click **OK** to confirm the action. The report definition is deleted.

Copying and Pasting a Management Report Definition

You can copy and paste a report definition. The report definition settings are pasted to the new location with the exception of the **report Targets** setting.

Note: If you copy a report definition from one group container to another, the **report targets** for the pasted report are automatically reset to include all of the children of the container into which the report is pasted. After pasting a report, you should edit the report definition properties to be sure that the assigned **report targets** are appropriate to the new report context and your overall reporting plan.

Use the following steps to test the copy and paste of a report definition.

To copy and paste a report definition using the left menu:

1. Using the left menu, select the report definition element you want to copy and right-click to display the report element action menu.
2. Select the **Copy** option from the action menu.
3. Using the left menu, select the container or monitor element to which you want to add the copy of the report definition and right-click to display the action menu.
4. Select the **Paste** option from the action menu. The report definition is added to the container.
5. If necessary, edit the pasted report definition to verify the appropriate **report targets** are selected.

To copy and paste a report definition using the container Contents panel:

1. Using the left menu, select the container or element that contains the report definition you want to copy.
2. If necessary, click the **Contents** tab from the right panel view menu. The applicable Contents panel is displayed.
3. In the reports section of the Contents panel, click the check box to the left of the name of the report definition that you want to copy.

4 Click the copy icon button at the bottom of the reports section panel.

5 Using the left menu, select the container or element into which you want to paste the report definition.

6 If necessary, click the **Contents** tab from the right panel view menu. The applicable Contents panel is displayed.

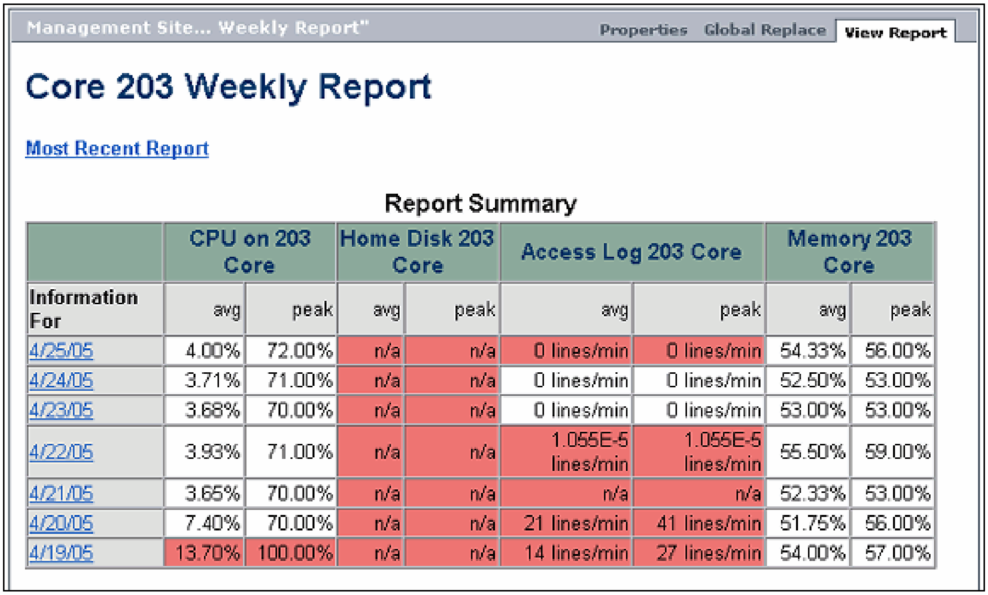
7 Click the paste icon on the container action menu at the top of the Contents panel. The report definition is added to the container.

8 If necessary, edit the pasted report definition to verify the appropriate **report targets** are selected.

Understanding the View Report Tab

You use the View Report tab to access reports that have been generated or to manually generate a report based on the selected report definition. The following section describe the features and actions available on the View Report tab.

The Report Summary table provides links to reports that have been generated for the selected report definition. The following figure is an example of the View Report tab showing the Report Summary table.



Core 203 Weekly Report

Most Recent Report

Report Summary

	CPU on 203 Core		Home Disk 203 Core		Access Log 203 Core		Memory 203 Core	
Information For	avg	peak	avg	peak	avg	peak	avg	peak
4/25/05	4.00%	72.00%	n/a	n/a	0 lines/min	0 lines/min	54.33%	56.00%
4/24/05	3.71%	71.00%	n/a	n/a	0 lines/min	0 lines/min	52.50%	53.00%
4/23/05	3.68%	70.00%	n/a	n/a	0 lines/min	0 lines/min	53.00%	53.00%
4/22/05	3.93%	71.00%	n/a	n/a	1.055E-5 lines/min	1.055E-5 lines/min	55.50%	59.00%
4/21/05	3.65%	70.00%	n/a	n/a	n/a	n/a	52.33%	53.00%
4/20/05	7.40%	70.00%	n/a	n/a	21 lines/min	41 lines/min	51.75%	56.00%
4/19/05	13.70%	100.00%	n/a	n/a	14 lines/min	27 lines/min	54.00%	57.00%

The left hand column in the table displays date-coded hyperlinks you use to view individual reports. The columns of the table list the monitors that are included in the report. Below each monitor name are two columns which summarize the average and peak measurements or values recorded for the period of the report. Entries highlighted in red or yellow indicate that the measurement exceeded the error or warning status threshold for the monitor.

Clicking the **Most Recent Report** link above the summary table displays the latest report available for the monitor or group.

At the bottom of the View Report tab is the **Generate** button. You click this button to generate a new report for the currently selected report definition regardless of when the report was normally scheduled to be generated.

Configuring Management Report Settings

A Management Report can be added to any SiteScope monitor group container or individual monitor in the monitor tree. You configure the report using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings and options you use to configure a Management Report.

Main Settings

You use the Main Settings section to select which monitors are included in the report, what data to include in the report, and select formatting options. Complete the Main Settings for the Management Report as described below.

Name

Enter a text description for this Management Report definition. This name is used to identify this Management Report definition in the product display.

Monitor and Groups to report on

Use the context menu tree to the right of this item to select the groups and/or monitors to be include in this report. The context menu includes the currently selected container and all of the child containers. By default, the current container and all child elements are selected. Check one or more individual elements to associate this report definition to the selected elements.

Thresholds

Check this option to create a table of monitor error, warning, and good threshold settings for all of the monitors included in the report. If selected, this table is displayed as the first report section.

Uptime and Readings

This option creates two report tables: **Uptime Summary** and **Measurement Summary**. These tables include the following:

Data in the Uptime Summary Table

- Name - the name of monitors included in the report
- Uptime % - the percentage of monitor readings reported as good
- Warning % - the percentage of monitor readings reported as warning
- Error % - the percentage of monitor readings reported as error
- Last - the last reading of the monitor for the report period

Data in the Measurement Summary Table

- Name - the name of monitors included in the report
- Measurement - the parameter being monitored (for error condition)
- Max - the maximum value recorded for the Measurement parameter during the report period
- Avg - the average value of the readings recorded for the report period
- Last - the last reading of the monitor for the report period

Uptime: Count warning good

Check this option to have any monitor readings that are reported as warnings included in the overall Uptime calculation.

Uptime: Remove warning

Check this option to suppress monitor readings reported as warnings from the overall Uptime and Readings Summary section. Note: This option only suppresses the display of the Warning % column in the table; it does not change the calculation of the Uptime %.

Uptime: Failure as good

Check this option to suppress monitor readings reported as errors from the overall Uptime and Readings Summary section. Note: This option only suppresses the display of the Error % column in the table; it does not change the calculation of the Uptime %.

Time in Error

This option creates a table summary listing each monitor selected for the report with a summary of how many minutes the monitor status was calculated as being in error for the period of the report.

Monitor Readings

Creates a table of individual readings recorded by the monitors during the report period, including all readings (error, good, and warning). This report table may also include blank "buckets" depending on the period of the report and how often the monitors ran during the period.

Errors

Creates a table of individual error readings recorded by the monitors during the report period.

Warnings

Creates a table of individual warning readings recorded by the monitors during the report period.

Goods

Creates a table of individual good readings recorded by the monitors during the report period.

Graph of Measurements

For **graph** reports, use the drop-down list to choose a graphical measurement to be included in the report. The options are described below.

Note: A bar graph is generated using standard HTML, so it can be printed from all browser types. Line graphs are generated using a java applet and may not print directly from all browsers.

- **None - no graph** Select this option to omit graphs from the report. The report only includes the tabular data contents you have selected.
- **Bar graph - one graph per measurement -** This bar graph option displays a single type of measurement per graph and per monitor during the specified time frame. For reports on multiple monitors, this results in the most number of graphs with one bar graph generated for each type of measurement for each monitor.
- **Line Graph - one graph per measurement -** This line graph option displays a separate line graph for each type of measurement for a single monitor. Like the bar graph option, this results in the most number of line graphs with one line graph generated for each type of measurement for each monitor selected for the report regardless of any compatibility of measurement type.
- **Line Graph - group per monitor instance -** This line graph option attempts to group all measurements from a single monitor instance into a single graph per monitor. The number of line graphs actually generated depends on whether the monitor records multiple measurements per monitor run (for example, the Windows Resources or UNIX Resources monitor types) and whether the measurement types are compatibility with one another. Separate graphs are generated if the measurement types are not compatible.
- **Line Graph - group same measurement types -** Select this option to plot the same measurement types gathered by several different monitor instances into single graphs. A line graph is generated for each set of compatible measurement types regardless of the number of monitors selected for the report.

- **Line Graph - group compatible measurements -** Select this option to display all compatible measurements from the selected monitors on a single graph. The option is intended to minimize the total number of line graphs generated. The number of graphs generated is still dependent on the compatibility of the selected monitor types and the measurement types collected by those monitors. If all of the monitors selected for the report are of the same type, for example URL monitors, then a single graph is generated with a colored line for each of the monitors.

Time Period for Report

Select the time period for which you want to view monitoring data. You may choose to report on data for a set number of hours, for the last day, or for the last several days, the past week, past month, or month-to-date for the current calendar month. Daily and month-to-date reports are generated every day at the scheduled time. Weekly reports are generated on Sundays at the scheduled time, and monthly reports are generated on the first day of the month following the current month so that they contain an entire month's worth of data.

Alert Table

Check this option to include a table of alerts sent for the monitors in the report. The options for the Alert Table level are:

- Basic
- Show Detail for Failed Alerts
- Show Detail for All Alerts

File Format

This option allow some customization of the report appearance. The options are:

- color background (default)
- color background, no table borders
- white background

Send Report by E-Mail

To have the report forwarded by e-mail when it is generated, enter the e-mail address(es) to which this report should be sent each time its generated. To send the reports to multiple e-mail addresses, separate the e-mail addresses with commas.

HTML Format

Select this option box if you want the reports sent in HTML format. Use this option to include the SiteScope report graphics. If you do not select this option only a text summary of the report is sent.

Format Template

Select a template for SiteScope to use to create the e-mail message. You can choose from the following templates or make a copy of one of these and customize it to meet your own needs.

- **HistoryLongMail -** Choose this option to send a detailed history report. It contains both user and administration links.
- **HistoryLongXMLMail -** Choose this option to send a detailed history report. It contains both user and administration links for reports & XML files.
- **HistoryMail -** This is the default option.
- **HistoryMailAlertDetail -** Choose this option to have all alerts included in the report that is e-mailed.
- **HistoryMailNoLinks -** Choose this option to send the report without any links in it.

Advanced Settings

Use the Advanced Settings to configure additional format, schedule, and content options for the Management Report. The following lists the advanced setting options for the Management Report.

Detailed monitor information

If this box is checked, the all of the information gathered for each monitor is displayed on the report. Otherwise, only the primary data is displayed for each monitor. For example, on a URL Sequence Monitor, if this box is checked, the timing information for each step in the sequence is displayed in the report.

Show Which Monitors

By default, the report shows data for all of the monitors in the report. You use this option to have only a subset of those monitors to be shown - those that have had the specified status something during the report's time frame. For example, choosing "show only monitors that had errors" displays report data only if that monitor had spent time in error sometime during the time interval of the report.

Schedule Filter

By default, the report shows data for the full period of the report. You use this option to have only a only a subset of the data to be shown - those monitors that have samples during the time period of the schedule. For example, choosing "weekdays, 9-6" displays report data for the selected monitors with samples inside the 9am to 6pm time period, Monday through Friday. Also, only this data is used for all the calculations.

Best Case Calculation

Check this option to calculate the monitor uptime percentage, warning percentage, and error percentage using a “best case scenario”. In this scenario, monitor time in error is calculated from the first monitor run that explicitly reported an Error instead of from the time of the last known Good monitor run.

Time Between Samples

Use this time scale option to choose the time interval between monitor readings. By default, SiteScope uses automatic scaling. When automatic scaling is used, SiteScope determines how many readings were taken over the chosen time period for the given monitors and then selects an appropriate interval for the management report. You use the Scale option to choose intervals that range from once every minute to once a day.

Max Value on Graph

You use the vertical scale option to choose the maximum value displayed on a graph. By default, SiteScope uses the maximum sample value. Choosing a specific scale value makes it easier to compare graphs from different monitors and times.

Description

Use this optional text field to describes other information about this report definition. For example, include information about the purpose, target, setup date, or audience for this report.

Disable

Select this box to temporarily disable the generation of this report. To enable the report again, clear the box.

End of Report Period

By default SiteScope generates reports starting at the indicated time and ending at the time the report was generated. You may choose an alternate end time by selecting a time from the drop-down list. For example, you may want to have your reports run from midnight to midnight.

Comma-delimited file

Select this box to save a generated management report to a comma-delimited text file which you can then import into a spreadsheet application.

SiteScope automatically saves these files in the **<SiteScope install path>/SiteScope/htdocs** directory. To find the exact location of the saved file on your machine, choose the Reports button on the SiteScope navigation bar and click the link for this report in the **Reports** column to go to the Report page. The full path to the file is listed in parenthesis directly next to the date line. If you enter an e-mail address in the **E-mail** text box, SiteScope sends a copy of the comma-delimited file to that address.

Note: The comma-delimited file creates two columns for each monitor reading, one containing the value with units, and the other containing just the value. This is to make it easier to import the comma-delimited data into a third party application which may not automatically separate data values from the text describing the units.

Send Comma-delimited file by E-mail

If you enter an e-mail address in the text box, SiteScope sends a copy of the file to that address.

XML file

Select this box to save a generated management report to an XML text file. SiteScope automatically saves these files in the <**SiteScope install path**>/**SiteScope/htdocs** directory. To find the exact location of the saved file on your machine, choose the Reports button on the SiteScope navigation bar and click the link for this report in the **Reports** column to go to the Report page. The full path to the file is listed in parenthesis directly next to the date link.

Note: The XML file creates two columns for each monitor reading, one containing the value with units, and the other containing just the value. This is to make it easier to import the XML data into a third party application which may not automatically separate data values from the text describing the units.

Send XML file by E-mail

If you enter an e-mail address in the text box, SiteScope sends a copy of the XML file to that address.

Generate report at

Indicate the time that you want SiteScope to generate this management report. The report contains information for the last day, week, or month, ending at the time the report is run. For example, if a daily report is generated at 18:00 (6:00 p.m.), it contains data generated between 18:00 the previous day and 18:00 of the current day. The default value is 00:00 which represents midnight.

Note: SiteScope Management report generation may temporarily impact overall SiteScope performance and responsiveness depending on the number of monitors and time period of the report. Generally, you should schedule reports to be generated during off-peak hours relative to overall monitoring tasks and load. If you are generating many reports each day, you should consider staggering the **Generate report at** value for different reports.

72

SiteScope Quick Report

You use the Quick Report form to create a one-time SiteScope management report for any time interval that is needed.

Working with SiteScope Quick Reports

You use SiteScope Quick Reports to view monitor data for any monitor, groups of monitors, and time period that you select. Quick reports are generated only on demand rather than automatically at regular intervals as with SiteScope Management Reports.

When you choose to generate a Quick report, SiteScope reads the applicable log files and generates the report based on the applicable monitor measurement information and the time interval you specify. The settings you select for the Quick report do not persist as a report definition in the SiteScope configuration data. This is to say that Quick reports are not added as objects in the left menu tree.

Note: The time interval for a Quick report is not incremented automatically. This means that a Quick report always contain the data for the absolute **Report Period** interval defined in the report definition. To view more recent data using a Quick report, you must edit the **Report Period** setting.

Note: When working in Business Availability Center, Quick Report definitions in System Availability Management Administration are stored only with the Business Availability Center context. Quick Report definitions are not stored in and do not persist on the SiteScope server.

Creating a Quick Report

Use the following steps to create a Quick report.

To create a new report definition:

1. Using the left menu, select the SiteScope monitor group container or monitor element to which you want to associate the report definition.
2. If necessary, click the **Contents** tab from the right panel view menu. The applicable Contents panel is displayed.
3. Click the **New Report** button at the top of the Contents view or at the bottom of the reports section of the Contents area. Alternately, you can right-click the container in the left menu to display the container action menu and select **New report**. The report selection page is displayed in the content panel.
4. Select the **Quick Report** link. The New SiteScope Report page for Quick reports is displayed.
5. Complete the items in the **Main Settings** as described in the section below. If necessary, complete the items in the **Advanced Settings** and other sections as described in the sections below.
6. When the required settings are defined, click the **Apply** button to create the report.

Configuring Quick Report Settings

Quick Report can be generated for any SiteScope monitor group container or individual monitor in the tree. You configure the report using the Properties panel which contains settings presented in collapsible panels. The report is generated when you click the **Apply** button at the bottom of the New SiteScope Report page.

The following sections describe the settings and options you use to configure a Quick Report.

Main Settings

You use the Main Settings section to select which monitors to include in the report, what data to include in the report, and select formatting options. Complete the Main Settings for the Quick Report as described below.

Monitors and Groups to report on

Use the context menu tree to the right of this item to select the groups and/or monitors to be include in this report. The context menu includes the currently selected container and all of the child containers. By default, the current container and all child elements are selected. Check one or more individual elements to associate this report definition to the selected elements.

Thresholds

Check this option to create a table of monitor error, warning, and good threshold settings for all of the monitors included in the report. If selected, this table is displayed as the first report section.

Uptime and Readings

This option creates two report tables: **Uptime Summary** and **Measurement Summary**. These tables include the following:

Data in the Uptime Summary Table

- Name - the name of monitors included in the report
- Uptime % - the percentage of monitor readings reported as good
- Warning % - the percentage of monitor readings reported as warning
- Error % - the percentage of monitor readings reported as error
- Last - the last reading of the monitor for the report period

Data in the Measurement Summary Table

- Name - the name of monitors included in the report
- Measurement - the parameter being monitored (for error condition)
- Max - the maximum value recorded for the Measurement parameter during the report period
- Avg - the average value of the readings recorded for the report period
- Last - the last reading of the monitor for the report period

Uptime: Count warning good

Check this option to have any monitor readings that are reported as warnings included in the overall Uptime calculation.

Uptime: Remove warning

Check this option to suppress monitor readings reported as warnings from the overall Uptime and Readings Summary section. Note: This option only suppresses the display of the Warning % column in the table; it does not change the calculation of the Uptime %.

Uptime: Failure as good

Check this option to suppress monitor readings reported as errors from the overall Uptime and Readings Summary section. Note: This option only suppresses the display of the Error % column in the table; it does not change the calculation of the Uptime %.

Time in Error

This option creates a table summary listing each monitor selected for the report with a summary of how many minutes the monitor status was calculated as being in error for the period of the report.

Monitor Readings

Creates a table of individual readings recorded by the monitors during the report period, including all readings (error, good, and warning). This report table may also include blank "buckets" depending on the period of the report and how often the monitors ran during the period.

Errors

Creates a table of individual error readings recorded by the monitors during the report period.

Warnings

Creates a table of individual warning readings recorded by the monitors during the report period.

Goods

Creates a table of individual good readings recorded by the monitors during the report period.

Graph of Measurements

For **graph** reports, use the drop-down list to choose a graphical measurement to be included in the report. The options are described below.

Note: A bar graph is generated using standard HTML, so it can be printed from all browser types. Line graphs are generated using a java applet and may not print directly from all browsers.

- **None - no graph -** Select this option to omit graphs from the report. The report only includes the tabular data contents you have selected.
- **Bar graph - one graph per measurement -** This bar graph option displays a single type of measurement per graph and per monitor during the specified time frame. For reports on multiple monitors, this results in the most number of graphs with one bar graph generated for each type of measurement for each monitor.
- **Line Graph - one graph per measurement -** This line graph option displays a separate line graph for each type of measurement for a single monitor. Like the bar graph option, this results in the most number of line graphs with one line graph generated for each type of measurement for each monitor selected for the report regardless of any compatibility of measurement type.
- **Line Graph - group per monitor instance -** This line graph option attempts to group all measurements from a single monitor instance into a single graph per monitor. The number of line graphs actually generated depends on whether the monitor records multiple measurements per monitor run (for example, the Windows Resources or UNIX Resources monitor types) and whether the measurement types are compatibility with one another. Separate graphs are generated if the measurement types are not compatible.

- **Line Graph - group same measurement types -** Select this option to plot the same measurement types gathered by several different monitor instances into single graphs. A line graph is generated for each set of compatible measurement types regardless of the number of monitors selected for the report.
- **Line Graph - group compatible measurements -** Select this option to display all compatible measurements from the selected monitors on a single graph. The option is intended to minimize the total number of line graphs generated. The number of graphs generated is still dependent on the compatibility of the selected monitor types and the measurement types collected by those monitors. If all of the monitors selected for the report are of the same type, for example URL monitors, then a single graph is generated with a colored line for each of the monitors.

Report Period

This option specifies the period of time that you want the report to cover. Enter the time from which you want the report coverage to start in the **From** boxes and the time to which you want to cover in the **To** boxes. Note that times should be entered in 24-hour format.

Report in

Select the format to be used in displaying the report: HTML format, Text format or XML format.

Alert Table

Check this option to include a table of alerts sent for the monitors in the report. The options for the Alert Table level are:

- No Alert Table
- Basic Alert Table
- Show Detailed Alert Table for Failed Alerts
- Show Detailed Alert Table for All Alerts

File Format

This option allow some customization of the report appearance. The options are:

- color background (default)
- color background, no table borders
- white background

Send Report by E-Mail

To have the report forwarded by e-mail when it is generated, enter the e-mail address(es) to which this report should be sent each time its generated. To send the reports to multiple e-mail addresses, separate the e-mail addresses with commas.

Advanced Settings

Use the Advanced Settings to configure additional format, schedule, and content options for the Quick Report. The following lists the advanced setting options for the Quick Report.

Detailed monitor information

If this box is checked, the all of the information gathered for each monitor is displayed on the report. Otherwise, only the primary data is displayed for each monitor. For example, on a URL Sequence Monitor, if this box is checked, the timing information for each step in the sequence will be displayed in the report.

Show Which Monitors

By default, the report will show data for all of the monitors in the report. You use this option to have only a subset of those monitors to be shown - those that have had the specified status something during the report's time frame. For example, choosing "show only monitors that had errors" will display report data only if that monitor had spent time in error sometime during the time interval of the report.

Schedule Filter

By default, the report will show data for the full period of the report. You use this option to have only a only a subset of the data to be shown - those monitors that have samples during the time period of the schedule. For example, choosing "weekdays, 9-6" will display report data for the selected monitors with samples inside the 9am to 6pm time period, Monday thru Friday. Also, only this data is used for all the calculations.

Best Case Calculation

Check this option to calculate the monitor uptime percentage, warning percentage, and error percentage using a “best case scenario”. In this scenario, monitor time in error is calculated from the first monitor run that explicitly reported an Error instead of from the time of the last known Good monitor run.

Time Between Samples

Use this time scale option to choose the time interval between monitor readings. By default, SiteScope uses automatic scaling. When automatic scaling is used, SiteScope determines how many readings were taken over the chosen time period for the given monitors and then selects an appropriate interval for the management report. You use the Scale option to choose intervals that range from once every minute to once a day.

Max Value on Graph

You use the vertical scale option to choose the maximum value displayed on a graph. By default, SiteScope will use the maximum sample value. Choosing a specific scale value will make it easier to compare graphs from different monitors and times.

73

Monitor Summary Report

The Monitor Summary Report provides you with detailed information about the monitors defined in one or more monitor groups.

Introducing the Monitor Summary Report

Use the Monitor Summary Report to view setup information on monitors as well as the organization and makeup of groups of monitors. For example, you can check and compare monitor run frequencies (the **Frequency** setting) if you are having problems with monitor skips. You can also use the report to check for monitor dependencies that can impact alerting. You can use the file export option to export the monitor configuration data to a third-party application such as a spreadsheet or text editor.

Monitor Summary Reports are ad hoc reports and their definitions are not stored for future use. No report element is added to the monitoring tree for this report type.

Generating a Monitor Summary Report

Use the following steps to generate a Monitor Summary Report.

To generate a report:

1. Using the left menu, select the SiteScope monitor group container or monitor element that encompasses all of the monitor and group elements you want to include in the Monitor Summary Report.
2. If necessary, click the **Contents** tab from the right panel view menu. The applicable Contents panel is displayed.
3. Click the **New Report** button at the top of the Contents view or at the bottom of the reports section of the Contents area. Alternately, you can right-click the container in the left menu to display the container action menu and select **New report**. The report selection page is displayed in the content panel.
4. Select the **Monitor** link. The New SiteScope Report page is displayed.
5. Complete the items in the **Main Settings** as described in the section below. To have the report results exported to an external file, complete the items in the **Advanced Settings** section as described below.
6. When the required settings are defined, click the **Apply** button to create the report. The report output is displayed in a new browser window. If you selected to have the report output to an external file, the link to the file is displayed in a new browser window.

Configuring Monitor Summary Report Settings

A Monitor Summary Report can be generated for any SiteScope monitor group container or individual monitor in the monitor tree. You configure the report using the Properties panel which contains settings presented in collapsible panels. The following sections list the settings and options you use to configure a Monitor Summary Report.

Main Settings

You use the Main Settings section to select which monitors are included in the report, what data to include in the report, and select formatting options. Complete the Main Settings for the applicable report type as described below.

Monitor and Groups to report on

Choose the monitors or groups of monitors that you want to include in the report. By default, all of the children of the selected node are included in the report. Use the expandable tree menu feature to view the monitors within the selected context. Use the check boxes to the left of the monitor names to select or deselect monitors to include in the report.

Display Columns

Choose the monitor information to display in the report columns. Hold down the shift key to select a set of adjacent groups. Use CTRL-click to select non-adjacent items. Data is shown in the report for the selected parameters only if the particular option has been selected, such as **Disabled** and **Frequency**, or if a value has been supplied, such as Monitor Descriptions. If the option or value has not been defined in the particular monitor setup, the column is blank for that parameter for that monitor.

Sort By

Choose the monitor parameter to use as a sort key for the report. For example, to have report sorted alphabetically by monitor type, select Monitor Type. Select the applicable radio button below the list box to have the report sorted in **Ascending** or **Descending** order using the selected sort key.

Show Parameters

Select this box if you want the report to contain the parameters defined for each monitor. This option includes a list of the active options defined for each selected monitor in a single table cell rather than individual columns as with the option above.

Advanced Settings

Use the Advanced Settings to select options for exporting the report. The following lists the advanced setting options for the Monitor Summary Report.

Export to File

Select this box to have SiteScope export the Monitor Summary report data to an text file.

File Name

When the **Export to File** option is enabled, SiteScope writes the data to the filename specified in the **File Name** box using the selected text format. The file is written into the **<SiteScope install path>/SiteScope/htdocs** directory. If you do not specify a filename, the default file name is "monSummary.csv" and the default file format is comma-separated text.

File Format

Use the drop down menu to select the format for the exported file. The options are comma-delimited text, tab delimited text, or HTML.

Reading the Monitor Summary Report

The Monitor Summary Report is presented in a table format. The columns that are displayed are determined by the **Display Columns** selected in the Monitor Summary Report Form. Data in the report include information about the configuration and current settings of monitors in the groups you have selected to include in the report.

Below is an example of a Monitor Summary Report for the Server group running on Windows. The report example shown includes the following:

- The group name to which the monitor belongs
- The display name or text description for each monitor
- The frequency at which the monitor is set to run
- Whether or not the monitor is disabled
- The schedule, if any, used to enable or disable the running of this monitor

A description of the other parameters defined for the monitor, such as disk drive, content match expression, and so forth.

Group	Monitor	Frequency	Disabled	Schedule	Parameters
Server	CPU	1 hour			
Server	Disk space on C	1 hour			Disk: C
Server	Disk space on D	2 hours			Disk: D
Server	Memory	1 hour			
Server	Microsoft IIS	1 hour			Web Server: Microsoft
Server	World Wide Web Publishing Service	30 minutes			Service: World Wide Web Publishing Service

Part VIII

SiteScope Advanced Information

74

Using Regular Expressions

Several SiteScope monitors allow for content matching on the text returned from a monitor's request or action (see the documentation for each monitor for more information about the content returned). This adds an important level of functionality in system monitoring. SiteScope makes use of regular expressions to match text content.

Using Regular Expressions in SiteScope

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

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

Defining a Regular Expression

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

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

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

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

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

  The following sections describe many of the different elements and patterns that can be used for creating regular expressions for content matching.

Matching String Literals

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

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

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

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

Using Alternation

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

Matching Patterns with Metacharacters

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

Metacharacters Used in Regular Expressions

Metacharacter	Description
\s	Matches generic white space (that is, the Spacebar key). This metacharacter is particularly useful when combined with a quantifier to match varying numbers of white space positions that may occur between words that you are looking to match.
\S	Matches characters that are NOT white space. Note that the \S is capitalized versus the small \s used to match white space.
.	This is the period or dot character. Generally, it matches all characters . SiteScope considers the dot as a form of character class on its own and therefore it should not be included inside the square brackets of a character class.
\n	Matches the linefeed or newline character.
\r	Matches the carriage return character.
\w	Matches non-white space word characters, the same as what is matched by character class [A-Za-z0-9_]. It is important to note that the \w metacharacter matches the underscore character but not other punctuation marks such as hyphens, commas, periods, and so forth.

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

Defining Character Classes

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

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

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

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

Example Character Classes

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

Using Quantifiers

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

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

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

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

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

Search Mode Modifiers

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

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

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

Regular Expression Match Mode Modifiers

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

Retaining Content Match Values

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

For example, if the content match expression was

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

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

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

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

```
2007
```

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

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

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

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

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

SiteScope Date Variables

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

General Date Variables

The following table lists the general variables:

Variable	Range of Values
$hour$	0 - 23
$minute$	0 - 59
$month$	1 - 12
$day$	1 - 31
$year$	1000 - 9999
$shortYear$	00 - 99
$weekdayName$	Sun - Sat
$fullWeekdayName$	Sunday - Saturday
$0hour$	00 - 23
$0minute$	00 - 59
$0day$	01 - 31 (two-digit day format)
$0month$	01 - 12 (two-digit month format)

Variable	**Range of Values**
$monthName$	Jan - Dec (three-letter month format in English)
$fullMonthName$	January - December
$ticks$	milliseconds since midnight, January 1, 1970

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

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

and the content returned by the request includes the string:

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

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

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

For example, if the current day is June 1, 1998, and the search expression is:

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

the content string that would match would be:

```
Updated on 06/02/98
```

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

Language/Country Specific Date Variables

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

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

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

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

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

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

and the content returned by the request includes the string:

```
mercredi
```

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

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

```
/$fullWeekdayName_fr$/
```

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

Special Substitution for Monitor URL or File Path

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

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

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

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

the log file for the following day would be:

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

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

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

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

SiteScope monitor types that support the special substitution are:

- eBusiness chain
- File Monitor
- Log Monitor
- URL Monitor
- URL Sequence Monitor
- Web server monitor

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

Examples for Log File Monitoring

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

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

Matching Comma-Separated Values

The following is an example of log file entries that are comma-separated strings of digits and letters:

```
new,open,changed,12,alerts
new,open,changed,13,alerts
new,open,changed,13,alerts
new,open,changed,14,alerts
```

A regular expression to match on log file entries that are comma-separated strings of digits and letters.

```
/([\w\d]+,[\w\d]+,[\w\d]+,[\w\d]+)[\n\r]?/
```

Note: If the file entries include punctuation marks such as an underscore or a colon, add that character explicitly to the [\w\d] class pattern. For example, to include a colon character, change each of the [\w\d] patterns to [\w\d:].

Matching Whitespace Separated Values

The following is an example of log file entries that are a sequence of strings and digits separated by spaces:

```
requests 12 succeeded 12 failed
requests 12 succeeded 12 failed
requests 11 succeeded 11 failed
requests 12 succeeded 12 failed
requests 10 succeeded 10 failed
```

The following is a regular expression to match on log file entries that are a sequence of strings and digits separated by spaces.

```
/([\w\d]+\s+[\w\d]+\s+[\w\d]+\s+[\w\d]+\s+[\w\d]+)[\n\r]?/
```

Note: The use of the + character forces the match to include the number of sequences per line included in the match pattern: in this example, five word or number sequences per line of the log file. If the sequences include punctuation marks such as an underscore or colon, add that character explicitly to the [\w\d] class pattern. For example, to include a colon character, change each of the [\w\d] patterns to [\w\d:].

Matching and Retaining the Numbers in a Line of Text and Numbers

The following is an example of log file entries that are comma separated strings that combine digits and letters:

```
request handle number 12.56, series 17.5, sequence reported 97.45, 15.95 and 19.51

request handle number 15.96, series 27.5, sequence reported 107.45, 25.95 and 19.52

request handle number 11.06, series 36.5, system codes 9.45, 35.95 and 19.53

log reference number 12.30, series 17.5, channel reset values 100.45, 45.95 and 19.54
```

The following is a regular expression to match on log file entries that are comma-separated strings that combine digits and letters and retain the decimal numeric data:

```
/[,\w\s]+(\d+\.\d+)[,\w\s]+(\d+\.\d+)[,\w\s]+(\d+\.\d+)[,\w\s]+(\d+\.\d+)[,\w\s]+(\d+\.\d+)[\n\r]
?/.
```

Note: If the file entries include punctuation marks such as an underscore or colon, add that character explicitly to the [,\w\s] class pattern. For example, to include a colon character that appears embedded in the text sequences, change each of the [,\w\s] patterns to [,:\w\s].

Matching Integers and Floating-point Numbers (Positive or Negative)

The following is an example of log file entries that are a sequence of integers and floating point numbers that may be negative or positive:

```
12.1987 -71 -199.1 145 -1.00716
13.2987 -72 -199.2 245 -1.00726
14.3987 -73 -199.3 345 -1.00736
15.4987 -74 -199.4 445 -1.00746
```

The following is a regular expression to match on log file entries that are a sequence of 5 integers and floating point numbers that may be negative or positive. The numbers in each entry must be separated by one or more spaces.

```
/(-?\d+\.?\d{0,})[\s]+(-?\d+\.?\d{0,})[\s]+(-?\d+\.?\d{0,})[\s]+(-?\d+\.?\d{0,})[\s]+(-
?\d+\.?\d{0,})[\n\r]?/
```

Matching Date and Time Coded Log Entries

Many log files include some form of date and time data with each entry. The following is an example of log file entries that include date and time information together with string data separated by commas:

```
20/04/2003 14:29:22,ERROR,request failed
20/04/2003 14:31:09,INFO,system check complete
20/04/2003 14:35:46,INFO,new record created
```

The following is a regular expression to match on log file entries that are date- and time-coded followed by comma-separated strings of letters and digits. This example uses the SiteScope date variables to match only on entries that were created on the same day, month, and year as indicated by the system clock of the server where SiteScope is running.

```
/$0day$\/$0month$\/$year$\s+\d+:\d+:\d+,[\w\d]+,[\w\d]+/
```

The following example uses the SiteScope date variables to match on a more restricted set of entries that were created on the same day, month, year, and within the same hour as indicated by the system clock of the server on which SiteScope is running.

```
/$0day$\/$0month$\/$year$\s+$0hour$:\d+:\d+,[\w\d]+,[\w\d]+)/
```

Some Pitfalls in Working with Regular Expressions

The most significant problem that has been seen with regular expressions in SiteScope is the use of the .* construct. This match construct presents a very large number of possible matches on any page of content. The use of the .* construct is known to cause the regular expression-matching engine used by SiteScope to take over all available CPU cycles on the SiteScope server. If this occurs, SiteScope is unable to function and must be restarted each time the monitor with the offending regular expression is run, until the expression has been corrected.

Note that regular expression matching is run against the entire text content returned to the SiteScope monitor request. As mentioned above, this includes HTTP headers that are normally not viewable in the browser window (for example, not visible using the **View** > **Source** option). This also means that you need to account for other information that may not be displayed in the browser view. This includes text in META tags used by Internet search engines as well as client side-scripts.

In the case of URLs that contain client side-scripts, such as Javascript, the text matching is done against the code lines of the script and not against the browser's output from the script. This means that if the script dynamically writes or replaces text on the Web page with values calculated by the script, it may not be possible to match this content with regular expressions. If the script is only changing text, you may be able to match the corresponding text strings that appear in the script code. A further pitfall would be that you are trying to check that a certain condition was met in the browser but the matching text string appears in the script content regardless of any user action.

Also note that a regular expression match succeeds as soon as the minimum match requested is satisfied. After a match is made, no further matching is performed. Therefore, regular expressions are not well suited to count the number of occurrences of a repeating text pattern. For example, if you want to check a Web page with a catalog list of items and each item has a link next to it saying Buy Now! and you want to make sure that at least five items are listed, a regular expression of /Buy Now!/ would succeed in matching only the first Buy Now!. Likewise, if your regular expression searches the word catalog on the main browser screen, the match may succeed if the word appears as a META tag in the HTML header section or if it appears as a hyperlink in a site navigation menu that appears in the content before the occurrence you intend to match.

Another pitfall is forgetting to account for non-alphanumeric content. As mentioned above, regular expressions need to be written to account for all of the characters that are and may be present. This includes white space, linefeed, and carriage returns. This is not normally a problem when matching a single-word literal. It can be a challenge when you need to create a match of several words separated by unknown amounts of white space and other non-alphanumeric characters and possibly span more than one line. The [\s\n\r]+ character class can be useful between words used in the expression. Always check the format of the content you are trying to match to look for patterns and special characters, such as periods, commas, and hyphens, that may cause a seemingly simple match to fail.

The use of excessive metacharacters can lead to frustration. In some cases, overly generous quantifiers combined with the . or \W metacharacters can grab content that you were intending to match with a literal string elsewhere in your regular expression resulting in a match failure. For example, the following might be used to match the URL content of the hyperlink anchor reference: /a href="([\W\w\s]*)"/. When the monitor performs the check for this regular expression, however, the match grabs the first occurrence of the pattern /a href="... and continues matching multiple lines of text up to the last quotation mark found on the page. Without some other unique ending delimiter, the [\W\w\s]* class and quantifier combination is too excessive. A more successful syntax that narrows the class of expected characters would be: /a href="?([:\/\w\s\d\.]*)"?/

The following are some examples of syntax for use in regular expressions:

Example Expression	Description
/CUSTID\s?=\s?([A-Z0-9]{20,48})/	This example matches an ID string that is made of 20 or more digits and upper-case letters with no spaces or other non-alphanumeric characters. The \s? construct allows a white space on either side of the equals sign. Using the parentheses around the character class instructs SiteScope to retain this value (up to the maximum of 48 characters) as a content match value and the matched value is displayed in the monitor detail status column.
/a href="?([:\/\w\s\d\.]*)"?/i	This example matches the URL string in an HTML hyperlink. The "? construct makes a quotation mark on either end of the URL string optional. Using the parentheses instructs SiteScope to retain this value as a content match value and the value is displayed in the monitor status. The i modifier tells the search to treat upper- and lower-case letters equally.
/"[^"]*"/	This example matches text sequences that are contained between quotation marks. Note the use of the negation caret (^) to define a character class of all characters other than the quotation mark.

As with programming and scripting languages, there is almost always more than one way to construct a regular expression to accomplish a particular match. There is not one right way to build regular expressions. You should plan to test and modify regular expressions as necessary until you get the results you need.

For an in-depth discussion of Perl regular expressions, consult a book about Perl programming, or find a Perl tutorial on the Web.

75

Monitoring XML Documents

SiteScope's content matching capabilities is an important feature in monitoring networked information systems and content. For SiteScope monitors that provide content matching, the basic content matching is available through the use of Perl regular expressions. SiteScope also includes the capability of matching document content by traversing XML documents. For example, you can include an XML match content string using the URL Monitor and Web Services Monitor to match an XML element name, an attribute of an XML element, or the content of an element. You can use this to check for content in XML based Web pages, SOAP or XML-RPC documents, and even WML pages served to WAP-enabled devices.

Understanding Content Matching for XML Documents

The syntax of XML match content strings reflects the hierarchal structure of the XML document. Match content strings that start with "xml" are recognized as element names within an XML document. The element names are added, separated by periods, in the order of their relationship to the root element. For example, in the document weather.xml the root element is <weather>. This element includes child elements named <area>, <skies>, <wind>, <forecast>, and so forth. To access the content of these XML elements or their attributes, you would use a syntax like xml.weather.area.

To check that specific content or value is present, add an equals sign after the element name whose content you are testing and then add the value of the content. If there are multiple instances of an element name in the document, you can check a particular instance of that element by adding the number indicating the order of the element in the document in square brackets (see the example in the table below). You can also test for multiple elements or values by separating individual search strings with commas. The table below gives several examples of the syntax used to match content in XML documents.

Example Match Content	Description
xml.weather.temperature	Succeeds if any <weather> node in the document contains **one or more** <temperature> elements. The content of the <temperature> elements is returned by the monitor. If no <temperature> element is found within the <weather> node, an error is returned.
xml.weather.temperature=20	Succeeds if any <weather> node in the document contains **one or more** <temperature> elements where the content of the <temperature> element equals 20. The content of the <temperature> element is **NOT** returned by the monitor if the match is found. An error is returned if no <temperature> element is found within the <weather> node or if no <temperature> element contains the value 20.

Example Match Content	Description
xml.weather.forecast.[confidence]	Succeeds if any <weather> node in the document contains a <forecast> element that has an **attribute** called confidence. The value of the confidence attribute is returned by the monitor if the match is found. An error is returned if no <forecast> element is found within the <weather> node or if no confidence attribute is found.
xml.weather.forecast[3].[confidence]=50	Succeeds if any <weather> node in the document contains three or more <forecast> elements where the third <forecast> element has a confidence **attribute** with a value of 50. An error is returned if the <weather> node has fewer than three <forecast> elements or if the value of the confidence attribute is not equal to 50.
xml.weather.temperature=20, xml.weather.skies=rain	Succeeds if any <weather> node in the document contains **one or more** <temperature> elements where the content of the <temperature> element equals 20 **AND** if any <weather> node contains **one or more** <skies> elements where the content of the <skies> element equals rain. Returns an error if either of the matches fails.
xml.wml.card.p.table.tr.td.anchor=Home Page	Checks the content of <anchor> elements in the designated path of a WML document. Succeeds if any <card> node containing table cells with **one or more** <anchor> elements where the content of any of the <anchor> elements equals "Home Page."

Using XML Content Match Values in Monitor Configurations

Monitors like the URL Monitor have a content match value that is logged to the SiteScope monitor data log and can also be used to set error and warning status thresholds for the monitor. The values of the XML names are saved as the content match values for the monitor.

For example, if the match content expression was xml.weather.temperature and the document was the contents of the file weather.xml, then the content match value would be 46.

You can then set the error, warning, and good status thresholds in the Advanced Options section for the monitor to compare your specific thresholds to the value returned by the content match.

For example, if you were monitoring temperature values and wanted to be alerted when the temperature value dropped below 72 degrees, you could set the monitor status thresholds as follows:

Error if	content match < <= 72
Warning if	content match == <= 72
Good if	content match >= > 72

With this configuration, the monitor would check the content of the temperature element and then compare it to the error and warning thresholds. In the example above, the status of the monitor would be an **error** because the temperature value is 46, which is less than 72.

76

Writing Scripts for Script Alerts

This chapter describes how to write automated system recovery scripts for use with the SiteScope Script Alert.

About Writing Scripts for Script Alerts

SiteScope has the ability to execute scripts or batch files when an error or warning status is detected. This is normally done by creating a Script Alert that acts as a trigger for the script. The script or batch file can execute any system command or call other programs written in any language. You can use this to create recovery scripts to automatically respond to critical conditions or failures.

Working with Scripts in SiteScope

The script file that a SiteScope Script alert is to execute must be located in the **<SiteScope install path>/SiteScope/scripts** directory or in the **<SiteScope user home>/scripts** directory on a remote UNIX machine (for remote scripts). For example, if SiteScope is installed in the directory C:\SiteScope and your script is called actionTest.bat, SiteScope tries to execute the following command line in response to Script Alerts you have created:

```
C:\SiteScope\scripts\actionTest.bat C:\SiteScope\scripts monitor_name
```

where C:SiteScope\scripts is the first command line parameter, monitor_name is the second command line parameter, and so forth.

Note: While the local script executed by the Script Alert must reside in the **<SiteScope install path>/SiteScope/scripts** directory, the execution path is the **<SiteScope install path>/SiteScope/classes** directory. You should use full path names for any file system commands or programs called by the script to avoid problems with defining the current execution directory.

The action taken by a script is determined by the creator of the script. SiteScope passes several command line arguments to each script called by a Script Alert. You can use this to have program scripts take action based on information sent from SiteScope. By default, SiteScope passes the following parameters to each Script alert as command line arguments:

- The path name of the scripts directory.
- The name of the monitor that caused the alert.
- The current status of the monitor.
- The path name to the alert message file.
- The Id code of the monitor.
- The group in which the monitor is located.
- Any additional parameters specified in the **Parameters** box in the alert form.

These command line arguments can be accessed by the target script using the normal command line variable conventions. These conventions are %1, %2, %3 and so forth, for Windows NT systems, and $1, $2, $3 and so forth, for UNIX scripts (depending on the scripting shell or language used). The first six parameters (that is, %1 through %6) are passed by default to each script. To pass other parameters, the property variables or parameters must be added to the Script Alert Settings in the Parameters box to make them available to the script. The first variable or text entered in the Parameters box is then accessible as %7 by the script, the second parameter is accessed as %8, and so forth.

An example script written in Perl to access Script Alert parameters:

```
print "pathname to scripts directory: $ARGV[0]\n";
print "name of monitor causing alert: $ARGV[1]\n";
print "current status monitor: $ARGV[2]\n";
print "pathname to alert message file: $ARGV[3]\n";
print "id code of monitor: $ARGV[4]\n";
print "group for the monitor: $ARGV[5]\n";
```

The following is an example batch file for Microsoft Windows to echo the parameters passed to the script:

```
echo pathname to scripts directory: %1
echo name of monitor causing alert: %2
echo current status monitor: %3
echo pathname to alert message file: %4
echo id code of monitor: %5 echo group for the monitor: %6
```

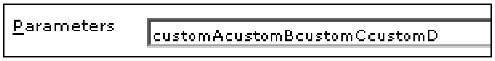
Passing Data from SiteScope to a Script

In addition to the seven default parameters, there are two other mechanisms for passing parameters and data to scripts. One is to use the additional Parameters box in the Script Alert Settings. The other is to access the Alert Message file.

Passing Data Using the Script Alert Settings

The simplest way to send additional custom parameters and data to script is to use the Alert Action wizard. The seventh default parameter passed to the script, which is any additional parameters specified on the alert form, allows you to specify one or more custom parameters to be sent to the script. You specify these in the **Parameters** box in the Script Alert Settings on the Action Types Settings Page of the Alert Action wizard.

These parameters could be hard-coded values. You can include multiple parameters by separating the individual parameters by spaces. For example, assume you want to pass the four text strings shown below to a script. To do this you enter them in the Parameters box as follows:



Parameters: customAcustomBcustomCcustomD

These would then become the seventh (7th) through tenth (10th) command line parameters sent to the script. The following Windows batch file script would print the default parameters as well as the additional example custom parameters entered in the Parameters box of the Action Types Settings Page:

```
echo pathname to scripts directory: %1
echo name of monitor causing alert: %2
echo current status monitor: %3
echo pathname to alert message file: %4
echo id code of monitor: %5
echo group for the monitor: %6
echo seventh parameter(customA): %7
echo eighth parameter(customB): %8
echo ninth parameter:(customC) %9
echo tenth parameter(customD): %10
```

Passing Data Using the Alert Message File

The other method for passing data and SiteScope monitor parameters to a script is to use the Alert Message file. This is a file that is created by SiteScope using the alert template specified in the Alert Action wizard. You can create your own custom alert templates and pass custom text strings or any of the SiteScope parameters available. The following shows the default NTEventLog template included with SiteScope. The parameters marked with < > brackets are replaced with the applicable values to and written to the Alert Message file each time the applicable Script Alert is triggered.

```
The NTEventLog Script Alert Template
Type: <eventType>
Event Time: <eventTime>
Source: <event>
Source ID: <eventID>
Category: <eventCategory>
Machine: <eventMachine>
Message: <eventMessage>
Monitor: <name>
Group: <group>
Sample #: <sample>
Time: <time>
<mainParameters>
<mainStateProperties>
```

To use this data in a script, your script needs to access the Alert Message file at the pathname location specified by the fourth default command line parameter (see “Working with Scripts in SiteScope” on page 1312). Then the script has to parse the content of the Alert Message file to extract the data you want to use in your script.

For more examples of how to write recovery scripts, look at the script files in the <**SiteScope install path**>/**SiteScope/scripts** directory. You can use the **actionTest.bat** example template to create your own script. The **perlTest.pl** example shows how to call a Perl script. The **restartIIS.bat**, **restartService.bat**, and **restartServer.bat** scripts implement common recovery actions.

For the UNIX environment, the examples scripts are called action **Test.sh** and **perlTest.pl**.

77

Customizing Alert Templates

This chapter describes how to customize SiteScope alert templates to alter the content and format of alert messages.

About Alert Templates

An important part of effectively managing your network infrastructure is having access to accurate, up-to-date, and specific information about the condition of systems and servers. You use SiteScope alerts to send notification of system faults and errors when they are detected. You can customize SiteScope alert templates to meet specific requirements of your organization.

SiteScope uses templates when generating alert messages and reports. In most cases, you select the template you want to use in the Define Alert form when you create an alert. You can customize the existing templates or create your own by making a copy of an existing template. You customize the alert templates by adding or removing text, by adding property variables as listed in the Template Properties section, or changing the order of text or property variables that are included in the template.

Note: It is recommended that you create custom alert templates using new filenames. If you modify one of the default templates provided with SiteScope and save the changes to the same file, the changes that you make may be lost if you reinstall SiteScope or upgrade the SiteScope installation.

Alert Template Groups

To make a custom alert template available to SiteScope, you must save any customized alert templates into the directory containing the templates for the applicable alert type. The following is a list of the directory names containing SiteScope alert templates you can copy and customize.

Template Group	Description	Location
Event Log	Format and content of data written into event logs	**<SiteScope install path>/ SiteScope/templates.eventlog**
History	Format and content of e-mail messages that notify recipients that a report has been generated	**<SiteScope install path> / SiteScope/templates.history**
E-Mail	Format and content of alert messages sent by e-mail	**<SiteScope install path>/ SiteScope/templates.mail**
Template	Group Description Location Pager Format and content of pager alerts	**<SiteScope install path>/ SiteScope/templates.page**
Post	Format and content of messages submitted to a CGI script by a Post alert	**<SiteScope install path>/ SiteScope/templates.post**

Template Group	Description	Location
Script	Format and content of messages sent to a script when a script alert is triggered	**<SiteScope install path>/ SiteScope/templates.script**
SNMP	Format and content of messages sent by SNMP when a SNMP trap is triggered	**<SiteScope install path>/ SiteScope/templates.snmp**

The templates in these groups are text files that include property variable markers. You use a text editor to create or modify these templates. The new templates saved into the directories shown become available to the applicable alert on the Define Alert form.

The following is an example of the default template used for the E-mail Alert. The names that appear within <brackets> are property variable markers. When the alert is generated, SiteScope replaces these markers with the corresponding values of the variable for the monitor or monitor group that has triggered the alert.

```
This alert is from SiteScope at <SiteScopeURL>
Monitor: <groupID>:<name>
Group: <group>
Status: <state>
Sample #: <sample>
Time: <time>
----------------------Detail ---------------------
<mainParameters>
<mainStateProperties>
```

You add or edit the text portions of the template. For example, you could change the first line of the template above to read:

```
A Web monitoring alert was generated by the SiteScope installation found at
<SiteScopeURL>
```

To change the text content of alert messages

1. Open a text editor that has access to the alert template directories on the SiteScope machine.
2. Open one of the existing template files in the template directory of the alert type you want to customize. For example, to customize an alert template for use with E-mail alerts, select a template file in the **<SiteScope install path>/SiteScope/templates.mail** directory.
3. Make changes to the template. Depending on the alert type, you can add or remove text, change the order of text or property variables, or add other property variables. To add specific monitor results or monitor configuration properties, add the applicable property variable name between < > bracket pairs to the template. The Template Properties section contains lists of the available properties for different monitor types. For example, to add the percentage of a disk drive that is full for an alert used for Disk Space monitors, add the property variable <percentFull> to the template.
4. Save the changes to a unique filename within the directory for the applicable alert type.

   You can customize Sound alerts by adding your own audio files for SiteScope Sound alerts. The files must be of the ***.au** format.

Other Template Groups

The following table shows other template types used by the SiteScope application. The templates in these directories are reserved, and are not used by alerts.

Note: You should not modify the templates in these directories without specific procedures provided in the product documentation or as instructed by Customer Support.

Template Group	Description	Location
MIB	Text used with SNMP traps	**<SiteScope install path>/SiteScope/templates.mib**
Operating System	Shell commands to be executed when monitoring remote UNIX servers	**<SiteScope install path>/SiteScope/templates.os**
Performance Monitor	Used for NT performance monitoring	**<SiteScope install path>/SiteScope/templates.perfmon**
Sound	Audio files used for sound alerts	**<SiteScope install path>/SiteScope/templates.sound**
View	Query and XML/XSL templates	**<SiteScope install path>/SiteScope/templates.view**

78

UNIX Operating System Adaptors

This chapter includes information on how to create and customize adapter files to enable SiteScope monitoring of different versions of the UNIX operating system.

Working with SiteScope UNIX Operating System Adapters

You can use SiteScope UNIX operating system adapters to extend SiteScope to connect to, and remotely monitor other versions of UNIX, in addition to those supported by default. This is done by configuring an adapter file to support the particular version of UNIX you want to monitor.

SiteScope uses adapter files to describe the commands that are needed to retrieve a variety of system resource information from servers running different versions of the UNIX operating system. These adapter files are written in plain text and are stored in the **SiteScope/templates.os** directory. The default UNIX adapters that are provided with SiteScope include:

Filename	Description
AIX.config	Adapter file for IBM AIX
Digital.config	Adapter file for Digital Tru64 UNIX (Pre 4.x)
FreeBSD.config	Adapter file for FreeBSD 3.x
HP.config	Adapter file for Hewlett-Packard HP/UX
HP64.config	Adapter file for Hewlett-Packard HP/UX 64-bit
Linux.config	Adapter file for Linux (Redhat and others)
MacOSX.config	Adapter file for Apple MacIntosh OS X
OPENSERVER.config	Adapter file for SCO OpenServer
SCO.config	Adapter file for SCO UNIXWare
SGI.config	Adapter file for Silicon Graphics Irix
Sun.config	Adapter file for Sun Microsystems Solaris
Tru64.config	Adapter file for Compaq Tru64 UNIX 5.x

You can modify existing adapter files to adjust for specific system requirements in your environment. You can also create your own adapter files to enable SiteScope monitoring of other UNIX versions.

Adding an Adapter

You can add an adapter to specific versions of UNIX.

To add a UNIX adapter:

1. Read the Adapter Kit documentation thoroughly.
2. If the UNIX platform to which you want to add support is similar to one of the default SiteScope-supported UNIX platforms, make a copy of the adapter file for that UNIX version and use that as a starting point for your adapter.
3. Modify the adapter file to match the command line requirements for the UNIX version to which you want SiteScope to connect.
4. Save your adapter file to the **SiteScope/templates.os** directory. The filename must use the **.config** extension.
5. Open the installation SiteScope to which you have added the new adapter file.
6. In the left pane, expand **Preferences**. Right-click **UNIX Remote Preference**, and select **New UNIX Server**. The New UNIX Server page opens.
7. In the **OS** field, select the name of the UNIX adapter that you have created.
8. Click **OK**. SiteScope uses the new adapter file to try and retrieve that applicable data from the remote server.
9. If you make changes to the adapter file after you have configured one or more server connection profiles to use the adapter, you can use the **Detailed Test** option in the UNIX Remote Preferences to test your adapter. After adding the remote server, the Detailed Test displays the output of the command that SiteScope is running remotely, along with SiteScope's parsing of the output.

   The amount of work required to modify a particular template depends upon how different the new UNIX platform is from the supported UNIX platforms.

Adapter File Format

Each UNIX platform supported for remote monitoring by SiteScope has an adapter file in the **SiteScope/templates.os** directory. These files use SiteScope's standard setting file format.

The first group of settings (those settings before the first # sign line) describe the platform:

```
id=yourPlatform
name=your Platform Name
```

The id is the SiteScope internal ID for the OS. This ID must be unique, contain no spaces, and can be alphanumeric. It is recommended that you use the name of the adaptor file as the ID name. For example, if the name of your adaptor file is linux.config, your ID would be linux.

The name is the name you want displayed in the drop-down list when adding or editing remote servers.

The rest of the template file contains groups of settings representing a single command, separated by a line of # characters. For example, the following settings represent the disk space command:

```
id=disks
command=/usr/bin/df -k
mount=6
name=1
```

Where:

id=disks is the id that SiteScope uses to look up a command. This must be one of the set of SiteScope commands (see "Adapter Command List" on page 1327). This entry is case sensitive.

command=/usr/bin/df -k means that the usr/bin/df -k command is executed to get the information about the disks.

mount=6 and name=1 mean that the mount name is in column 6 and the name of the mount or file system is in column 1. The data names vary from command to command and are documented below.

Applying the above for the following command output:

```
Filesystem kbytes used avail capacity Mounted on /proc 0 0 0 0%
/proc /dev/dsk/c0t3d0s0 73049 42404 23341 65% /
```

where the disks command automatically skips lines not starting with (/dev) reads column 1 (/dev/dsk/c0t3d0s0) as the name of the file system, and column 6 ("/") as the mount name.

Adapter Command List

SiteScope requires settings for each the following commands to operate properly. Each command description requires an ID and a command, one or more fields to specify where the data is being read from, and optionally a set of modifiers that are used to filter the output of the command to eliminate certain sets of lines (such as header lines).

Where the variable column is used below, it means the number of the column in which the data appears, where columns are space delimited sets of data.

In addition, there are certain fields that can be optionally applied to any command description. For details, see “Optional Adapter Command Details” on page 1330.

Disk Listing

ID	Description	Used by	Fields
disks	Returns a list of the file systems on the system. The /usr/bin/df -k command is the standard way to get this data. Lines returned that do not start with /dev are automatically skipped.	Disk Space Monitor	➤ **name**. The column of the name of the file system. ➤ **mount**. The column of the name of the mount.

Disk Information

ID	Description	Used by	Fields
disk	Takes a disk as an argument and returns the total, free, and percent used for the disk.	Disk Space Monitor	➤ **total**. The column of the total kilobytes capacity of the file system. ➤ **free**. The column of the free kilobytes of the file system.

Memory

ID	Description	Used by	Fields
memory	The amount of swap spaced used and available.	Memory Monitor	➤ **swapUnit**. The multiplier applied to used, free, or total swap space to give bytes. ➤ **used**. The amount of swap space used. ➤ **free**. The amount of swap space free. ➤ **total**. The amount of total swap space. **Note:** Only two of used, free, and total fields need to read. The other is computed.

Page Faults

ID	Description	Used by	Fields
pageFault	The number of page faults/sec. If multiple page faults lines are matched, they are added up.	Memory Monitor	➤ **pageFaults**. The column of the number of page faults. ➤ **inPageFaults**. The column of the number of page in faults. ➤ **outPageFaults**. The column of the number of page out faults. ➤ **units**. pages (default), pages/sec, or k/sec units for the paging data. ➤ **pageSize**. If units are k/sec, the **pageSize** is used to compute the number of pages. Otherwise it is ignored. **Note:** Either use **pageFaults**, if there is a single column of data, or **inPageFaults** and **outPageFaults**, if there are two columns of page fault data. **inPageFaults** and **outPageFaults** are added together to get the total page faults.

CPU Usage

ID	Description	Used by	Fields
cpu	Returns the wait and idle % of the CPU.	CPU Monitor	➤ **idle**. The idle % for the CPU. ➤ **wait**. The wait % for the CPU (optional).

Process List

ID	Description	Used by	Fields
process	A list of processes with long process names. Typically this is /usr/bin/ps -ef	Service Monitor	**name**. The column of the names of the processes.

Process List with Details

ID	Description	Used by	Fields
process Detail	A list of processes with size of the process. Typically this is /usr/bin/ps -el	Service Monitor (with Check Memory option enabled)	➤ **name**. The column of the names of the processes ➤ **size**. The column of the size of the processes. ➤ **pageSize**. Page size on the system (optional). The default is 8192.

Optional Adapter Command Details

The following fields can optionally be applied to any command description:

Process List with Details

ID	Description
startLine	The line number where the command starts looking for data.
endLine	The line number where the command ends looking for data.
skipLine	The pattern that if matched, skips the line.
matchLine	The pattern that if matched, looks for data in that line.
startMatch	The pattern that if matched, starts the command looking for data.

ID	Description
endMatch	The pattern that if matched, ends the command looking for data.
reverseLines	If true, the command output lines are reversed and read back to front. This is useful if there is data at the end of the command and it is too difficult to work out when to start reading.

If a field name has the format, fieldnameColumnName=COLUMN, the adapter searches the headers (first line) for COLUMN and records the columns containing the data, and then use those settings to read the fieldname field. This is useful where the width of the columns varies, and the data has spaces in it.

For example, to read the my data information from the following command output:

```
MEM NAME DESC
12K my data some of my data
```

you would specify the name field in the command description as:

```
nameColumnName=NAME
```

The adapter reads the header line, finds NAME, and records where the previous column ends (MEM in this case) and where the specified column ends (NAME), and uses that to read, in this case, the text in character columns 6 through 22.

To see an example of the ColumnName reading in action, look at the process and processDetail commands for the supported UNIX platforms. They use this method to get the process name and the size of the process.

79

SiteScope Monitoring Using Secure Shell (SSH)

SiteScope supports a number of security capabilities. One of these is support for remote server monitoring using Secure Shell (SSH) connections. You can use SSH to connect to a server and automatically send a command, so that the server runs that command and then disconnects. This is useful for creating automated processing and scripting.

SiteScope and SSH

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely accessing a remote computer. It is widely used by network administrators to remotely control Web and other kinds of servers. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by encryption. Secure Shell client machines make requests of SSH daemons or servers on remote machines.

Monitoring with SiteScope over SSH has the following basic requirements:

1. The servers that you want to have monitored by SiteScope using SSH need to have a SSH daemon (or server) installed and active.
2. The machine on which SiteScope is running needs to be configured with an SSH client.

Possibilities and issues involved in using SSH for SiteScope Monitoring include:

- Beginning with the 7.8.1.1 release of SiteScope, there are two SSH client options for use on the server or machine on which SiteScope is running. SiteScope now includes a SSH client written in Java and native to the SiteScope application code. This client eases the setup of SSH connections and generally uses fewer system resources than external SSH clients.
- SiteScope for Windows also ships with a copy of the PuTTY SSH client and utilities. The PuTTY SSH client, plink.exe, has been used to enable SSH connectivity for SiteScope for Windows prior to the 7.8.1.1 release. SiteScope for Solaris and Redhat Linux make use of the SSH utilities normally bundled with those operating systems or available for download.

SSH Connectivity Options

The following table outlines the SSH connectivity options currently supported with SiteScope. For important information about configuring and managing SSH connectivity, see "Guidelines and Limitations" on page 1336.

SiteScope Platform and Client Options	Monitored Server Platform and Daemon
Windows PuTTY SSH client (included with SiteScope) or SiteScope integrated Java SSH Client	**UNIX/Linux** SSH host daemon (sshd - either proprietary or OpenSSH)
UNIX/Linux SSH client (/usr/local/bin/ssh or usr/bin/ssh) or SiteScope integrated Java SSH Client	**UNIX/Linux** SSH host daemon (sshd - either SunSSH, proprietary or OpenSSH)
Windows PuTTY SSH client (included with SiteScope) or SiteScope integrated Java SSH Client	**Windows** 1. SSH server (Cygwin OpenSSH, F-Secure, or OpenSSH for Windows 2. RemoteNTSSH package (included with SiteScope), to be installed into the appropriate directory on the remote server)

Guidelines and Limitations

- There are two different versions of the SSH protocol: version 1 and version 2. Version 1 and version 2 are different protocols and are not compatible with each other. This means that the SSH clients and SSH hosts must be configured to use the same protocol version between them to communicate. In many cases, SSH version 1 (SSH1) is the default version used. Some security vulnerabilities have been found in SSH version 1. Also, the SSH1 protocol is not being developed anymore and SSH2 is considered the current standard. We recommend using SSH version 2 (SSH2) for all SSH connections.

- The release version number of the SSH utilities and libraries you have installed must not be confused with the version of the SSH protocol that you want to be using. For example, OpenSSH release 3.5 supports both SSH1 and SSH2 protocols. The release version 3.5 does not mean that the libraries use an SSH version 3.5 protocol. You must configure the OpenSSH software to use either SSH1 or SSH2.

- If you have set up SiteScope remote monitoring using SSH connections and then make configuration changes or upgrades to the SSH daemon or server software deployed on remote servers in the environment, it may be necessary to reconfigure the SSH connectivity between the machine on which SiteScope is running and the remote servers that are being monitored.

- The availability of the Integrated Java SSH Client is indicated via the drop-down menu in the **SSH Connection Method** of the Advanced Settings section of the Remote UNIX Server and Remote Windows Server Properties page. If the option for Internal Java Libraries does not appear in the list, you can still use the Plink external SSH Client for SSH connections. You can also contact an HP sales representative to upgrade to a later version of SiteScope that includes the Integrated Java SSH Client.

Configuring Remote UNIX Servers for SSH Monitoring

SiteScope for Solaris or Linux supports remote monitoring via SSH. Setting up the SSH hosts on the remote servers you want to monitor in the UNIX environment can be very complex and is beyond the scope of this document. Some suggested resources on installation of the OpenSSH daemon are http://www.sunfreeware.com/openssh.html (for Solaris) and http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/ref-guide/s1-ssh-configfiles.html for Redhat Linux.

Configuration Requirements

The following are requirements for configuring remote UNIX servers for SSH monitoring with SiteScope in a UNIX environment:

- Secure Shell daemons or servers (sshd) must be installed on each remote server you want to monitor with SiteScope.
- The SSH daemons on the remote servers must be running and the applicable communication ports must be open. For example, the default for SSH is port number 22.
- A SSH client must be installed on the server where SiteScope is running. The SiteScope integrated Java SSH client normally fills this requirement.
- If you use an external SSH client on Solaris or Linux, the SSH client binaries must be accessible to SiteScope. When SiteScope invokes the SSH client process, it searches in both **/usr/bin** and **/usr/local/bin** for the ssh command. The ssh binaries must be in one of these two locations and SiteScope must have permissions to execute the ssh command.

  You should verify SSH client-to-server connectivity from the machine where SiteScope is running to the remote machine you want to monitor. You should check SSH connectivity outside of the SiteScope application before setting up remote server connections using SSH in SiteScope. For example, if SiteScope is running on Solaris or Linux, use the following command line to request an SSH connection using SSH2 to the server <remotehost>:

```
ssh -2 <remotehost>
```

This normally returns text information that indicates the version of SSH protocol that is being used. Also, this attempts to authenticate the current user. Use the -l username switch to request a login as a different user.

For SiteScope running on Windows, see the section on “Testing SSH connectivity with PuTTY utilities” on page 1361 for information about testing SSH connectivity outside of the SiteScope application on Windows NT/2000 machines.

Once you have confirmed SSH connectivity, create or configure UNIX Remote settings in SiteScope to use SSH as the connection method.

Configuring Remote Windows Servers for SSH Monitoring

The default remote connection method used by SiteScope for Windows-to-Windows connectivity and monitoring in Windows NT/2000/2003 networks is NetBIOS. While this has provided ease of connectivity, it does have several disadvantages. One is that NetBIOS is relatively vulnerable in terms of network security. Another is that it does not support remote execution scripts. Running commands on remote servers requires that scripts be executed locally with commands to the remote machine being written using the UNC syntax of remote servers. Even then, some parameters are not returned from the remote server via NetBIOS.

Starting with version 7.8, SiteScope supports monitoring of remote Windows NT/2000 servers using SSH. This technology has been tested with the OpenSSH binaries from Cygwin available at http://www.cygwin.com/ installed as the SSH server on the remote server. It has also been tested with the server available from F-Secure. You may also try OpenSSH for Windows (formerly Network Simplicity "OpenSSH on Windows") which is available on SourceForge.

The following is a comparison overview of two of the packages.

OpenSSH Package	Advantages	Disadvantage
Cygwin OpenSSH	1. Provides access to either Windows or UNIX-style scripting on a Windows machine. 2. Provides access to UNIX-style system tools and utilities. 3. SiteScope can access the remote server both as a Windows Remote and /or a UNIX Remote.	Complicated setup procedure.
OpenSSH for Windows	Simple setup procedure.	Only provides access to Windows commands, scripts, and utilities.

Note: OpenSSH for Windows and the Cygwin SSH implementations are incompatible with each other. They should not be installed on the same machine.

Note: If there is more than one version of the Cygwin utilities or more than one SSH server installed on a machine, there may be conflicts that prevent the SSH connections from working. An error message such as could not find entry point is one indication of this kind of conflict. If you suspect this error, search the machine for multiple copies of cygwin1.dll. It may be necessary to remove all versions of the utilities and then reinstall only a single installation to resolve this problem.

There are two main steps for configuring remote Windows Servers for SSH monitoring with SiteScope:

1. Installation and Configuration of a SSH Server

2. Installation of SiteScope Remote NT SSH Files

The following sections describe the steps you use to install the necessary packages:

1. Installation and Configuration of a SSH Server

To enable SiteScope monitoring using SSH, a SSH server must be installed and configured on each remote server to which you want SiteScope to connect. There are two software packages generally available that enable SSH capability. One is the Cygwin environment available from RedHat at http://www.cygwin.com/. Another package is the OpenSSH for Windows available at OpenSSH for Windows. The following describes the steps to install either of these packages:

Note: These setup steps must be performed for each server that runs the SSH daemon or server.

Installing Cygwin OpenSSH on Windows

Perform the following steps to install and configure a Cygwin OpenSSH server on Windows servers.

Important: The following instructions assume that no other Cygwin or other ssh utilities are installed on the machine and that the machine has Internet access.

Note: The user login account used to install and run the SSH daemon needs adequate permissions to install the necessary programs, configure several file options, and control Windows services. It does not need to be the account that SiteScope uses to connect to the subject server, although that account must be configured within the Cygwin installation before you can monitor that server with SiteScope.

To install and configure a Cygwin OpenSSH server on Windows NT/2000 servers:

1. Create a new System Environment variable with the following definition: CYGWIN = ntsec tty.
2. Add the string ;C:\cygwin\bin to your PATH variable. Save the changes to the variables.
3. Download the Cygwin setup program into a temporary folder. For example: C:\temp. The setup program is used to select, download, and install different packages and components available with Cygwin.
4. Run the downloaded setup program and choose the **Install from Internet** option when prompted to Choose A Download Source. Click **Next** to continue.
5. If prompted, select a root install directory where the Cygwin package should be installed. This is where the SSH daemon and related files are installed. For example, C:\cygwin. Click **Next** to continue.
6. If prompted, select a temporary directory where the Cygwin installation files should be stored. For example, C:\temp. Click **Next** to continue.
7. If prompted, select an Internet Connection option. Normally, **Direct Connection** can be used. Click **Next** to continue.
8. Select a suitable mirror site from which to retrieve the files using the selection list when prompted. Click **Next** to continue.

9 The Setup program queries the mirror site for the packages available and displays a hierarchy tree of package categories. To view and select the packages to download, click on the plus (+) symbol to the left of the category name to expand any of the package trees. Packages that are selected for download and installation display a version number in the **New** column. If a version number is not displayed for a particular package, it is not downloaded and installed. Click **Skip** to the left of package name to select the package for download.

Note: Many of the development (Devel) and database (Database) tools that may be selected by default for download are not necessary to run the SSH daemon and can be deselected to reduce download time and installation space.

Select each of the following packages for download and installation:

- cygrunsrv from the Admin branch
- cygwin-doc from the Doc branch
- pdksh from the Shells branch
- openssh and openssl from the Net branch
- your choice of UNIX-style text editor from the Editors branch (for example: vim or emacs)

Then click to download the files as prompted.

10 Depending on your installation options, the Cygwin setup downloads and installs the selected packages. You may be prompted to choose to have a shortcut to the Cygwin terminal window added to the Desktop or Program Start menu. Click to continue and complete the installation.

11 After the Cygwin setup is complete, open a Cygwin terminal window by clicking on the **Cygwin** desktop shortcut or Program Start menu item.

Note: Depending on the user profile in the Windows system, the default directory that opens in the terminal window may not be within the root Cygwin installation tree. Use the pwd command to display the current directory. Typing in the command string cd / normally changes the directory to the Cygwin root, which by default corresponds to the Windows C:\cygwin directory.

Update the default Cygwin group file with the group names in use on the machine and on your network. Use the mkgroup utility to update the default Cygwin group file with the groups defined on the server and in your domain. Examples of the commands to use are as follows:

```
mkgroup -l >> ../etc/group
mkgroup -d >> ../etc/group
```

Note:

- To have Cygwin recognize both domain and local group accounts, run the mkgroup utility twice, once for local users (-l option) and once for domain users (-d option). Remember to use >> syntax and not just >, to append entries to the file.
- If you use both the local and domain options, you must manually edit the /etc/group file (using the UNIX style text editor you downloaded) to remove any duplicate group entries. You may also want to remove group entries that are not needed for monitoring or should not have access to this machine.

Update the default Cygwin user (passwd) file with the users defined on the local machine plus any individual domain users you want to grant access to Cygwin on this machine. Use the mkpasswd utility to update the default Cygwin user file.

Examples of the commands to use are as follows:

```
mkpasswd -l >> ..\etc\passwd
mkpasswd -d -u username >> ..\etc\passwd (domain users)
```

Note:

- By default, Cygwin is set to run the OpenSSH daemon as the local user called SYSTEM. To have Cygwin recognize both domain and local machine user accounts, run the mkpasswd using the -l option to add all local users, and run it with the -d and -u options to add individual domain users. Remember to use >> syntax and not just >, to append entries to the file.
- If you use both the local and domain options, you must manually edit the /etc/passwd file (using the UNIX style text editor you downloaded) to remove any duplicate user entries. You may also change the default /home path and default shell for individual users. This may be necessary to install the RemoteNTSSH package in the /home/sitescopeaccount/ directory of the user account to be used by SiteScope.

12. Change the active directory to the /bin directory by typing cd /bin.
13. Create a symbolic link in the /bin directory that points to the Windows Command (CMD) shell by entering the following command line (be sure to include the trailing space and period):

    ```
    ln -s /cygdrive/c/winnt/system32/cmd.exe .
    ```

14 It is recommended that you change permissions and ownership of several Cygwin files and directories. Also create a log file for the SSH daemon. Type the following command lines in the Cygwin terminal command line and press ENTER after each command line entered:

```
cd /
chmod -R og-w .
chmod og+w /tmp
touch /var/log/sshd.log
```

Note:

- Exact syntax is required, including spaces.
- Inconsistent and incorrectly assigned file and directory permissions can be one reason that the SSH daemon can not be started or that SiteScope is unable to connect to and execute commands or scripts on the remote server.

15 Configure the SSH daemon to run as a Windows service by entering the following command:

```
ssh-host-config -y
```

When presented with the CYGWIN= prompt, enter ntsec tty to match the environment variable you set at the beginning of this procedure. Normally, this configures the SSH daemon or service to restart automatically if the server needs to be restarted.

16 Configure the encryption keys and files for the SSH daemon using the following command:

```
ssh-user-config -y.
```

Enter appropriate passphrases for several keystore files when prompted. The program asks you to re-enter the passphrase for confirmation.

17 You must change the ownership of several files and folders for use by the SSH daemon. The program does not normally run if the permissions on these files allow them to be changed or executed by group or "world" level users. Enter the following command strings to restrict access to these files:

```
chown SYSTEM:Users /var/log/sshd.log /var/empty /etc/ssh_h*
chmod 755 /var/empty
```

18 Check the installation by starting and then stopping the CYGWIN sshd service using the **Programs** -> **Administrative Tools** -> **Services** panel.

Note: Cygwin includes a server utility to start the SSH daemon. However, there have been a number of situations where this method failed to start the server, whereas using the Windows Services panel was able to start the server.

19 Configure the default shell or command environment for the user account you use for monitoring with SiteScope. The shell you select effects what types of scripts or commands can be run remotely using the SSH connection. Use the UNIX-style text editor and edit the /etc/passwd file. Find the entry for the SiteScope login account you intend to use and change the shell from /bin/bash to the shell you want to use as described below. This is normally the last entry in the line for that account entry.

a If you chose to have SiteScope interact with the remote server using the Windows Command shell, change the default shell entry to /bin/cmd. Use this option when you plan to use Windows-style batch files and scripts You must also include the symbolic link to the Windows cmd.exe kernel in the /bin directory as described in a previous step of this procedure.

b If you chose to have SiteScope interact with the remote Windows server using a Cygwin UNIX shell, change the default shell entry to be /bin/pdksh. The SiteScope SSH client may not accurately parse Cygwin's default bash shell. You must also configure a Remote UNIX server connection to this (Windows) server that connects to the Cygwin SSH daemon.

Save the changes to the file.

20 Edit the PATH and the default prompt commands in the /etc/profile file to ensure that Cygwin can find certain files and that SiteScope can parse the output from the remote shell. Use the UNIX-style text editor and edit the /etc/profile file. Find the PATH definition entry near the top of the file. For example:

```
PATH=/usr/local/bin:/usr/bin:/bin:$PATH
```

Change this to include the following:

```
PATH=.:/usr/local/bin:/usr/bin:/bin:$PATH
```

21 To change the default prompt commands, edit the /etc/profile file, and find the section similar to the following:

```
;;
sh  | -sh   | */sh  |\
sh.exe  | -sh.exe   | */sh.exe )
#Set a simple prompt
PS1='$ '
;;
```

Immediately under this entry, add the following:

```
;;
pdksh  | -pdksh   | */pdksh  |\
pdksh.exe  | -pdksh.exe   | */pdksh.exe )
#Set a simple prompt
PS1='> '
;;
```

22 Save the changes to the file.

23 Change the active directory to the home directory of the user you have created for SiteScope monitoring.

After making these changes and starting the SSH daemon, you should be able to connect to the server using an SSH client. For information about testing SSH connectivity outside of the SiteScope application on Windows NT/2000 machines, see the section on “Testing SSH connectivity with PuTTY utilities” on page 1361.

Note: Any time you run the mkpasswd -l /etc/passwd command (for example, when adding a new user), edit the /etc/passwd file again to make sure that the default shell for that user is set to the appropriate value for any account being used by SiteScope.

Installing OpenSSH for Windows

The OpenSSH for Windows package is an alternative to the Cygwin SSH package and can be easier to install. Like most products, the Cygwin product and the Open SSH for Windows are subject to change. There are cases where some versions of the Cygwin SSH server have not returned the data needed for SiteScope monitoring. If the OpenSSH for Windows package can solve this problem, you should use this package in place of the Cygwin package.

To install and configure an OpenSSH for Windows server on Windows NT/2000 servers:

1. Download and install the OpenSSH for Windows package.
2. Open a command prompt and change to the installation directory (C:\Program Files\OpenSSH is the default installation path).
3. Change the active directory to the OpenSSH\bin directory.
4. You must update the default group file with the group names in use on the machine and in your network. Use the mkgroup utility to update the default OpenSSH group file with the groups defined on the server and in your domain. Examples of the commands to use are as follows:

```
mkgroup -l >> ..\etc\group
mkgroup -d >> ..\etc\group
```

Note:

- To have OpenSSH recognize both domain and local group accounts, run the **mkgroup** utility twice, once for local users (-l option) and once for domain users (-d option). Remember to use >> syntax and not just >, to append entries to the file.
- If you use both the local and domain options, you must manually edit the /etc/group file (using the UNIX style text editor you downloaded) to remove any duplicate group entries. You may also want to remove group entries that are not needed or should not have access to this machine.

---

5 You must update the default OpenSSH user (passwd) file with the users defined on the local machine plus any domain user you want to grant access to the SSH server on this machine. Use the **mkpasswd** utility to update the default user file. Examples of the commands to use are as follows:

```
mkpasswd -l >> ..\etc\passwd
mkpasswd -d -u username >> ..\etc\passwd
```

Note:

- To have OpenSSH recognize both domain and local machine user accounts, run the **mkpasswd** utility using the -l option to add all local users and run it with the -d and -u options to add individual domain users. Remember to use >> syntax and not just >, to append entries to the file.
- If you use both the local and domain options, you must manually edit the /etc/passwd file (using the UNIX style text editor you downloaded) to remove any duplicate user entries. You may also change the default /home path and shell for individual users (see instructions below).

---

6 Check the installation by starting the **OpenSSH Server** service using the **Programs** > **Administrative Tools** > **Services** panel.

2. Installation of SiteScope Remote NT SSH Files

SiteScope includes a set of files that must be installed on each remote Windows server to enable certain commonly used server monitoring functions. The following sections describe the steps you use to install these files according to the SSH package you are working with.

To install the SiteScope SSH Files on Cygwin installations:

1 Verify that a **\sitescope_login_account_name** directory exists within the <**install_drive**>**:\cygwin\home** directory on each machine that is monitored by SiteScope using SSH. Replace **sitescope_login_account_name** with the user account name you use to connect to the machine using the SSH server.

2 One of the advantages of using SSH on Windows is that it allows SiteScope to execute scripts on the remote server running the SSH daemon. To be able to use the Script Monitor to run remote scripts, create a **scripts** subdirectory in the **/home/sitescope_login_account_name** directory. Scripts you create for execution by the SiteScope Script Monitor must be placed inside this directory.

3 On the machine where SiteScope is installed, find the file called **RemoteNTSSH.zip** in the <**SiteScope install path**>**\SiteScope\tools** directory.

4 Copy this file to the <**install_drive**>**:\cygwin\home\sitescope_login_account_name** directory on each of the remote Windows NT/2000 servers where you have installed the SSH server or daemon software.

5 Unzip the **RemoteNTSSH.zip** file on the remote server. Place the contents of the zip file into the <**install_drive**>**:\cygwin\home\sitescope_login_account_name** directory. This should create a <**install_drive**>**:\cygwin\home\sitescope_login_account_name\scripts** subfolder. You use this subfolder to hold scripts that can be run by the SiteScope Script Monitor.

6 Start the CYGWIN sshd service on the remote server.

Use the following steps to install the SiteScope SSH Files on OpenSSH for Windows installations.

To install the SiteScope SSH Files on OpenSSH for Windows installations:

1. On the machine where SiteScope is installed, find the file called **RemoteNTSSH.zip** in the <**SiteScope install path**>**\SiteScope\tools** directory.
2. Copy this file to the <**install_drive**>**:\WINNT** directory on each of the remote Windows NT/2000 servers where you have installed the SSH server or daemon software.
3. Unzip the **RemoteNTSSH.zip** file on the remote server. Extract the contents of the zip file into the <**install_drive**>**:\WINNT** directory. This should create an <**install_drive**>**:\WINNT\scripts** subfolder. You use this subfolder to hold scripts that can be run by the SiteScope Script Monitor.
4. Start the OpenSSH server service on the remote server.

After you have completed the steps above, it is recommended that you test SSH connectivity from your SiteScope server by using **plink.exe** or **PuTTY.exe** as described in the "Testing SSH connectivity with PuTTY utilities" on page 1361. After confirming SSH connectivity between SiteScope and the remote server, you can set up Remote Windows configurations as described in the User Guide, and select SSH as the connection method. You can then configure CPU, Disk, Memory Windows Performance Counter, and Script monitors to use the SSH connectivity.

SiteScope SSH Client Connection Options

After you have set up SSH servers or daemons on remote servers, you need to configure the SSH client that SiteScope uses to connect to the remote servers. As noted above, SiteScope includes two client options for SSH connectivity. The following presents an overview of the client options.

1. **Configuring SiteScope to use the integrated Java SSH client**

   SiteScope includes an integrated SSH client written in Java. This is the recommended option for SSH connectivity. One advantage of using this client option is that it uses fewer system resources than the external clients would use. Also, configuration of this client is simpler in some cases. To configure your remote using an external client, see "Using the Integrated Java SSH Client" on page 1354.

2. **Configuring SiteScope to use an external SSH client**

   SiteScope on Windows ships with a third-party SSH client called plink. Plink is one part of a set of SSH tools called PuTTY. SiteScope on UNIX and Linux require that an external SSH be installed on the machine where SiteScope is running. To configure your remote using an external client, see "Using an External SSH Client" on page 1358.

80

Working with SSH Clients

If you need to use Secure Shell (SSH) to connect to remote UNIX or Windows servers, SiteScope must have access to a SSH client to make the connection and transmit data. This section presents some of the client configuration possibilities and issues involved in using SSH for SiteScope monitoring.

Using the Integrated Java SSH Client

SiteScope provides a SSH client written in Java that is integrated into the SiteScope application. This client significantly reduces the required system resources used by SiteScope when connecting to servers via SSH. The Java client supports both SSH version 1 and version 2 protocols as well as both password-based and key-based authentication. The SiteScope configuration for the client is identical for UNIX, Linux, and Windows SiteScope. Documentation on using an external SSH client can be found at External SSH Client.

Working with the Integrated SSH Client

As noted previously, there are two different versions of the SSH protocol: version 1 and version 2. While they are both considered to be Secure Shell protocols, version 1 and version 2 are considered to be two different protocols and are not compatible with each other. Some security vulnerabilities have been found in SSH1. This resulted in several changes in SSH2, which is considered the current standard. Most SSH software supports both protocols. However, to be sure that a request for a SSH connection uses SSH2 instead of SSH1, it is necessary to configure SSH clients and SSH hosts to use the same protocol version between them to communicate. In many cases, SSH version 1 (SSH1) is the default version used for connections, as it is considered the lowest common denominator between a SSH client and a SSH host.

There are two ways to force SSH2 connections:

- Configure all SSH daemons or servers to accept only SSH2 connection requests.
- Configure the SSH client on the SiteScope server to only make SSH2 requests.

The first option is perhaps the most secure but may be the most time-consuming unless each server was configured for this option when it was installed and activated. The second option requires changes only to the client on the SiteScope server. For the integrated Java SSH client, this can be controlled by a setting in the SSH Advanced Options section on the remote server setup page.

Another part of SSH security is authentication. The integrated SSH client for SiteScope can be configured to use one of two authentication options:

- Password Authentication
- Key-Based Authentication

Password Authentication is the default method for SSH connections in SiteScope. Key-Based Authentication adds an additional level of security through the use of a passphrase and a public-private key authentication. For more details on how to set up key based authentication for SSH connections, see the following section titled Setting up Key-Based Authentication.

Setting up Key-Based Authentication

To use Key-Based Authentication for SSH remotes, you must first generate a pair of public/private keys. The public key resides on the remote and the private key is kept on the SiteScope machine. Both Cygwin OpenSSH and OpenSSH for Windows come with a key generation tool called ssh-keygen. The ssh-keygen tool allows you to create both protocol version 1 and version 2 keys. Read the documentation on ssh-keygen to create the type of key that you need.

When setting up a UNIX or Windows remote server using the Internal Java Libraries Client, use the key generation tool called MindTerm to create a public/private key pair for RSA (version 1 and version 2) and DSA (version 2). For example, to create a key pair using MindTerm:

To create a public/private key pair:

1 Launch MindTerm. Open a command window on the SiteScope server, and run the following command:

```
<SiteScope root directory>\java\bin\java -jar c:\<SiteScope root directory>\
WEB-INF\lib\mindterm.jar
```

Note: For SiteScope 7.9.5.x and earlier, enter the command: <SiteScope root directory>\java\bin\java -jar c:\<SiteScope root directory>\java\lib\ext\mindterm.jar.

2 In MindTerm, select **File** > **Create Keypair** > **DSA (or RSA)**. Also select OpenSSH .pub format.

3 The key pair is written to the <**USER_HOME**>**mindterm** directory. Copy the **identity.pub** file to the **SiteScope/groups** directory.

4 Copy the **identity.pub** file to the <**USER_HOME**>/**.ssh** directory on the remote machine and rename it **authorized_keys** (or **authorized_keys2** for SSH2).

5 On the remote machine, run the following command in the <**USER_HOME**>/**.ssh** directory, and make sure that User has read, write, and execute permissions, and that Group and Other have read permissions on the **authorized_keys** file.

6 Create a remote connection in SiteScope for the remote server using key file authentication and Internal Java Libraries.

The private key goes in the **SiteScope/groups** directory and the public key in the <**USER_HOME**>/**.ssh/authorized_keys** file on the remote machines.

The key generated from MindTerm is in **Openssh** format.

Note: You must verify that the server key and the MindTerm key are at the same level. For example, if the server key is 768 bit and the MindTerm key is 1024 bit, the authentication procedure fails.

To find out what your server is using:

1 Stop the sshd service on the remote server. On a Red Hat Linux server, run the command:

```
/etc/rc.d/init.d/sshd stop
```

2 Start the sshd service in debug mode on the remote server. On a Red Hat Linux server, run the command:

```
/usr/sbin/sshd -d
```

You should see output similar to `Generating 768 bit RSA key.`

Note: When using the **Key File for SSH connections** field in SiteScope, if there is a trailing space after the information entered, this causes an "unknown error (-1)" failure. Remove the trailing space to fix the problem.

Using F-Secure

The F-Secure client creates an SEC SSH formatted key and the F-Secure server understands a SEC SSH formatted key. To use the key generated using the Internal Java Libraries client (which is in openSSH key format), you must convert the openSSH key to SEC SSH format.

To convert the openSSH key to SEC SSH format:

1 Create a RSA key in MindTerm (which is an openSSH key pair).

2 Run the following command on the remote server to convert the openSSH key to SEC SSH format:

```
ssh-kegen -e -f <public key>
```

3 Leave the private key on the SiteScope server in the openSSH format.

Note: When using Key-Based authentication, the Key File supplied must be a version 2 private key.

Using SSH Version 2 protocol

By default, the SiteScope Java client uses the SSH1 Protocol if the server it is trying to connect to allows SSH1 connections. If this negotiation fails, SiteScope attempts to connect using version 2 protocol. The SiteScope Java client can be configured to use only SSH2 connections. Making the change on the SiteScope machine may be easier than having to reconfigure a large number of remote SSH servers.

When configuring your remote server profile, select the **SSH Version 2 Only** check box in the Advanced Settings.

Using an External SSH Client

SiteScope provides the capability of connecting to remotes using an external SSH client. On Windows platforms, the plink client is included with SiteScope. On UNIX and Linux platforms, SiteScope can use a standard SSH client such as SunSSH or OpenSSH.

Working with External SSH Clients

As noted previously, there are two different versions of the SSH protocol: version 1 and version 2. While they are both considered to be Secure Shell protocols, version 1 and version 2 are considered to be two different protocols and are not compatible with each other. Some security vulnerabilities have been found in SSH1. This resulted in several changes in SSH2 which is being considered the current standard. Most SSH software supports both protocols. However, to be sure that a request for a SSH connection uses SSH2 instead of SSH1, it is necessary to configure SSH clients and SSH hosts to use the same protocol version between them to communicate. In many cases, SSH version 1 (SSH1) is the default version used for connections, as it is considered the lowest common denominator between a SSH client and a SSH host.

There are two ways to force SSH2 connections:

- Configure all SSH daemons or servers to accept only SSH2 connection requests.

  This option is perhaps the most secure but may be the most time-consuming unless each server was configured for this option when it was installed and activated.

- Configure the SSH client on the SiteScope server to make only SSH2 requests.

  This option requires changes only to the client on the SiteScope server. For external SSH client, this is usually controlled via the client settings. For details on how to set the SiteScope PuTTY client to use SSH2, see "Setting up SSH2 on SiteScope for Windows Platforms" on page 1362.

Another part of SSH security is authentication. The integrated SSH client for SiteScope can be configured to use one of the following two authentication options:

- Password Authentication
- Key-Based Authentication

Password Authentication is the default method for SSH connections in SiteScope. Key-Based Authentication adds an additional level of security through the use of a passphrase and a public-private key authentication. See the following section for information on how to set up Key-Based authentication for SSH connections.

Monitoring with SSH on Windows Platforms

SiteScope for Windows platforms includes a SSH client to handle connections to remote SSH-enabled servers. SiteScope includes the PuTTY SSH utilities for SSH connectivity to both UNIX and Windows servers. These utilities are found in the <SiteScope install path>/SiteScope/tools directory.

By default, SiteScope SSH connections uses the SSH1 protocol (less secure) unless the server it is connecting to accepts only SSH2 sessions. To force SiteScope to use the SSH2 protocol (more secure), you need to configure the SSH client on the machine where SiteScope is running and possibly the SSH daemons/hosts on the remote servers to communicate using the SSH2 protocol. For SiteScope on Windows, configure the PuTTY SSH client utility and SiteScope as described in "Setting up SSH2 on SiteScope for Windows Platforms" on page 1362.

Note: The PuTTY and plink tools supplied with SiteScope are not the latest release versions of these tools. Starting with version 7.8.1.0, SSH connectivity is handled by the internal Java libraries by default. Consider checking for newer versions and replacing the files supplied with SiteScope with updated versions. More information about the PuTTY SSH client can be found at http://www.chiark.greenend.org.uk/~sgtatham/putty/ or http://www.openssh.org/windows.html.

Instructions for creating Public Keys using the PuTTYGen tool and using them are at http://the.earth.li/~sgtatham/putty/0.60/htmldoc/Chapter8.html#pubkey.

Note: SSH uses DES, BLOWFISH, RSA, or other public key cryptography for both connection and authentication. Public Keys are stored on a per-user basis so if you are using key-based logins instead of password-based logins, you should log in and run the PuTTYGen tool using the same account that is used by the SiteScope service.

Testing SSH connectivity with PuTTY utilities

It is recommended that you test SSH connectivity from SiteScope on Windows to remote hosts using either the PuTTY.exe or plink.exe tools. This is also useful for troubleshooting connectivity. You can use utilities to test connectivity with a SSH host. The plink utility is run from the command line.

To test SSH connectivity with PuTTY:

1. Log on to your Windows machine as the user who runs the SiteScope service.
2. Open a command window to the <**SiteScope install path**>**SiteScope****tools** directory.
3. Run the plink utility with the following syntax:

   ```
   plink -ssh <remoteuser>@<hostname>
   ```

   where <remoteuser> is the login username for a valid user account on the <hostname> server.
4. Follow the prompts in the terminal window to confirm that the remote login is successful. Log out of the terminal session when you are satisfied that the connection is working correctly.

   If you want to use the SSH2 protocol for connections, you need to use the PuTTY utility to configure the PuTTY client to use SSH2 instead of the default SSH1. This requires that you save session settings as described in the section "Setting up SSH2 on SiteScope for Windows Platforms" below. After you have done this, you can also use PuTTY to test SSH connectivity. You use the following steps for testing SSH2 connectivity using PuTTY:

To test SSH2 connectivity with PuTTY:

1. Log on to your Windows machine as the user who runs the SiteScope service.
2. Launch the PuTTY utility.
3. From the Session tab or tree, select the Saved Session name of the remote connection you want to test and click the **Load** button to the right of the selection box.

4 Click the **Open** button near the bottom of the dialogue box. This launches a terminal emulation window.

5 Follow the prompts in the terminal window to confirm that the remote login is successful.

6 Log out of the terminal session when you are satisfied that the connection is working correctly.

Setting up SSH2 on SiteScope for Windows Platforms

SiteScope for the Windows platform uses plink, part of the PuTTY suite of SSH tools, to create its SSH connections for remote monitoring. By default, the plink utility uses the SSH1 Protocol if the server it is trying to connect to allows SSH1 connections. The SiteScope SSH client can be configured to use only the SSH2 protocol for connections. Making the change on the SiteScope machine may be easier than having to reconfigure a large number of remote SSH servers.

Setting up SiteScope for Windows to use only SSH2 to communicate with remote UNIX or remote Windows servers requires two actions:

1 Create settings in the SSH client on the SiteScope server to use only SSH2.

2 Modify SiteScope remote server connection profiles to use the SSH2 connection profile.

The following two sections describe the steps you use to force SiteScope to use SSH2 for connecting to remote servers.

Use the following to steps to setup the PuTTY client on the SiteScope server to use only SSH2 by using the PuTTY utility suite.

To set up PuTTY to use SSH2:

1 Log on to the server where SiteScope is running as the user who runs the SiteScope service. To see which user this is, open the Services control panel, right-click the SiteScope service, select **Properties**, and click the **Log On** tab.

2 Find the **PuTTY.exe** tool in the **<SiteScope install path>\SiteScope\tools** directory. Alternatively, you can download an updated PuTTY version from the Internet.

3 Launch the PuTTY utility by double-clicking the icon in Windows Explorer (or typing **putty** in a command window with a path to the **<SiteScope install path>\SiteScope\tools** directory). No installation steps are needed. The Putty Configuration console opens.

4 With the **Session** tab or tree selected, enter the hostname or IP address of the remote machine to be monitored in the **Host Name** box. Select the SSH radio button below the hostname in the Protocol section.

5 Select the **Connection** tab or tree, and enter the username on the remote machine in the Auto-login username box. This should be a user account with permissions to monitor processes and hardware statistics on the remote server. Optionally, this user account might also have execution privileges to allow SiteScope to run scripts on the remote server.

6 Select the **SSH** tab or tree under the Connection tree, and then choose the **2** radio button in the Preferred SSH Protocol Version section.

7 Return to the Session tab. In the Saved Sessions text box, enter a name for these settings. Any previously saved settings appear in the list box below.

Note: The Saved Session name should not be a resolvable hostname on your network, nor can it contain a white space character. For instance, if these settings are for a machine named myhost.mydomain.com, the session settings name cannot be myhost, myhost.mydomain.com, or myhost settings (the latter is not allowed because of the white space between the words). Choose a name, such as myhost-settings.

8 Click the **Save** button. The name of your new settings should appear in the list of saved settings.

Repeat this process to create settings for each remote machine you wish to monitor with SiteScope using SSH2.

Note: Make a note of the Saved Session name for each machine that you configure, to enter this name into the SiteScope configuration file.

Configuring SiteScope to Use SSH2:

Use the following steps to configure SiteScope to use SSH2 for connecting to remote UNIX or remote Windows servers.

To configure SiteScope to use SSH2:

1. Open SiteScope in a Web browser. Click the **Preferences** node.
2. To setup SSH2 for a remote UNIX connection, click the **Unix Remotes Preferences** node. To setup SSH2 for a remote Windows connection, click the **Windows Remotes Preferences** node. The corresponding remote Servers page is displayed.
3. Click the **New Server** button for the type of remote server you are adding. The relevant New Server page is displayed.
4. In the **Host** box, enter the name of the settings you saved. For example, to use the settings for myhost.mydomain.com that were created above, you would enter myhost-settings in the box.
5. Select the applicable operating system of the target remote server in the **OS** drop-down list.
6. Leave the **Login** box blank.
7. Enter the password to log in to the remote machine in the **Password** box.
8. For UNIX Remotes: If the shell prompt for the remote UNIX server is something other than #, enter that prompt in the **Prompt** section.
9. For UNIX Remotes: Leave the **Login Prompt** and **Password Prompt** boxes blank.

10 Click **OK** to add the remote server profile.

Note: The remote connection test fails. You may see a message similar to the following error message:

```
Connecting to myhost-settings...
Waiting for prompt(#)...
Unable to open connection:
Host does not exist
Remote command error: unknown host name (-997)
```

Go to the <**SiteScope install path**>**SiteScope****groups** directory and make a backup copy of the **master.config** file. Rename the backup file to **master.config.SAV**.

---

11 Open the **master.config** file in a text editor, and locate the section of entries or lines beginning with the string _remoteMachine. If you have configured multiple remote server connections, there are multiple entries that begin with this string. Locate the line that includes the string _host=myhost-settings, where myhost-settings is the name of the host settings you entered in the Server Address box in PuTTY Configuration tool.

12 Add the following string to the end of that line:

```
_sshCommand=<SiteScope install path>\tools\plink.exe_-ssh_$host$_-pw_$password$
```

Note: This string must be entered on the same line. Do not add any carriage returns, new lines, or extra spaces.

Replace <**SiteScope install path**> with the path to your SiteScope installation. For example, if SiteScope is installed at C:\SiteScope, the string would read:

```
_sshCommand=C:\SiteScope\tools\plink.exe_-ssh_$host$_-pw_$password$
```

After you have finished making modifications, the entire line should look similar to the following example:

Note: This example wraps across multiple lines to fit on this page. When entering this setting into the SiteScope configuration file, be sure that it is entered all a single line.

```
_remoteMachine=_os=Linux _id=11 _trace= _method=ssh
_password=(0x)MGJJKDKLKJNINPNJMJ _login= _host=myhost-settings
_name= _sshCommand=C:\SiteScope\tools\plink.exe_-ssh_$host$_-
pw_$password$
```

13. Repeat this step to modify each _remoteMachine entry, using the applicable host name setting created for each host using the PuTTY Configuration tool in the previous section.
14. Save and close the **master.config** file.
15. Stop and restart the SiteScope service to force SiteScope to reload the manual changes you made to the **master.config** file.
16. Open a Web browser to the SiteScope server.
17. Click the **Preferences** node.
18. If you are setting up SSH2 for remote UNIX connections, click the **UNIX Remote Preferences** node. For SSH2 for remote Windows server connections, click the **Windows Remote Preferences node**. The corresponding Servers page is displayed.
19. For UNIX remotes, click the **Detailed Test** button in the Servers table for the UNIX Remote you configured to test the connection and verify that it works. For Windows remotes, click the **Test** button in the Windows Servers Table for the Windows Remote you configured to test the connection and verify that it works.

Note: This test normally takes a few seconds to complete.

81

Creating Custom Properties

The ability to customize SiteScope has been an important feature in extending and adapting it to a wide variety of environments and needs. This section describes how you can add custom property settings to SiteScope monitors and how you can add custom content to real-time Dashboard views in the SiteScope interface.

About Custom SiteScope Properties

Each monitor type in SiteScope includes a number of properties. You access these properties using the monitor's Properties view. You can add your own custom properties to SiteScope monitors. For details, see "Working with Custom Monitor Properties" on page 1368.

The Dashboard view displays real-time monitor results and related information in a table format. You can add a custom column for display in the Dashboard view. For details, see "Working with Custom Display Columns" on page 1373.

You can link custom properties to custom columns to have the values of your custom properties displayed in real-time SiteScope views. You can also have other SiteScope monitor properties displayed in custom columns. For details, see "Displaying Custom Properties in Custom Columns" on page 1375.

Working with Custom Monitor Properties

Each SiteScope monitor instance consists of a set of properties that define what action the monitor is to perform and how it is to perform these actions. Monitor properties also store information that may be passed to the system that is being tested.

The custom monitor property feature allows you to define and store additional information you associate with a monitor. For example, you may want to enable users to define property values that categorize monitors according to their importance, or actions that need to be taken if the monitor reports an error. You may add more than one custom monitor property to SiteScope.

Defining a custom monitor property adds a new form entry item to the add and edit view for monitors. A new form entry item is added for each custom property defined. The custom property definition fields are added to all monitor types.

Note: Custom monitor properties do not have default values and may be blank until you have defined a value for a property. Values are defined only when you explicitly enter or select a value and then update the monitor.

When you add a custom monitor property definition, SiteScope creates a new display panel in the monitor Properties view called Custom Property Settings.

Note: The Customer Properties area appears in the new interface even if no custom properties were defined for the SiteScope.

Custom Monitor Property Definition Syntax

Custom monitor property definitions are added as single line entries to the master.config file in SiteScope. The default custom property form element is a text box. You can also define a custom property to use selection menu entries. The syntax of the definition string for a custom monitor property that accepts plain text values is as follows:

_monitorEditCustom=*_propertyName*|*display_title*|*display_description*|*default _definition*

The syntax of the definition string for a custom monitor property that an option selection menu is as follows:

_monitorEditCustom=*_propertyName*|*display_title*|*display_description*|*default _definition*|*input_code*

The custom elements of the definition string are separated by the vertical pipe (|) symbol. The following table describes the elements of the custom property definition string:

Element	Description
_monitorEditCustom	The parameter name that signals SiteScope to add a custom monitor property to monitors.
_propertyName	The variable name for the property. Generally, this should begin with an underscore character to signal that it is a property variable. This name can be referenced elsewhere within SiteScope. Do not include spaces or punctuation marks as part of the property name.
display_title	The item title text to be displayed in the interface with the custom property entry or selection field. This string may include HTML markup code.
display_description	An optional text description to be displayed in the interface below the property entry field. Use this to describe the purpose and usage for the property. The string may include spaces and punctuation marks.
default_definition	An optional string to define a default value for the property. The default input object is a text field.
input_code	This field contains the HTML code for an option selection input object for setting the custom property value. This must include the $NAME$ and $VALUE$ special internal reference variables used by SiteScope to work with the list.

Note: The entire definition string must be on a single line of text. Do not insert any linefeeds or carriage returns in the definition.

It is not necessary to restart the SiteScope service to activate the custom properties. There may be a delay of several minutes for SiteScope to update its configuration data. Earlier versions of SiteScope required you to restart the SiteScope service to activate the custom properties.

You use the following steps to add a simple custom property:

To add a text or numeric custom property:

1. Make a backup of the master configuration file in a safe location. The file is found at **<install_path>\SiteScope\groups\master.config** on the machine where SiteScope is running.
2. Open the **master.config** file using a text editor.
3. Add a _monitorEditCustom= entry as a new line to the file.
4. On the same line, enter the text string to define the _propertyName, the display_title and the display_description. Separate each of the entries with the vertical pipe (|) symbol.
5. If you want to define a default value for the property, add the default value in the place of the input_definition entry.
6. Save the changes to the file.

To standardize custom property values, you can define a selection list as the input control. This allows you to define a set of values that can be assigned to a custom property. The following example defines a custom property named _actiongroup with an option selection menu having three options: SysDev, TestDev, and Production.

```
_monitorEditCustom=_actiongroup|Team|Select which support team has responsibility
for this monitor.|SysDev|<select name="$NAME$"><OPTION selected
value="$VALUE$">$VALUE$</option> <option>TestDev</option>
<option>Production</option></select>
```

Use the following steps to add an option selection list input control to a custom property definition.

To define a selection list input for a custom property:

1. Make a backup of the master configuration file in a safe location. The file is found at <**install_path**>**SiteScope****groups****master.config** on the machine where SiteScope is running.
2. Open the **master.config** file using a text editor.
3. Add a _monitorEditCustom= entry as a new line to the list of parameters.
4. On the same line, enter the string to define the _propertyName, the display_title and the display_description. Separate each of the entries with the vertical pipe (|) symbol.
5. For the input_definition item, enter the option selection code using the following syntax:

   ```
   <select name="$NAME$"><OPTION selected
   value="$VALUE$">$VALUE$</option>
   <option>option_value_1 Group</option>
   <option>option_value_2</option>
   <option>option_value_3</option>...</select>
   ```

   Where $NAME$ and $VALUE$ are required, internal reference variables and option_value_1, option_value_2, etc. are the text strings for the options in the selection menu.
6. Save the changes to the file.

Using Custom Properties in Alert Templates

You can reference custom monitor properties in alert templates. This allows you to include custom information about monitors in alerts sent by SiteScope. You use the _propertyName from the custom property definition as a variable reference in alert templates.

Working with Custom Display Columns

The Custom Column feature of SiteScope provides a flexible tool for customizing the information and functionality available through the SiteScope interface. The custom column can be used to display information as text, provide a hyperlink to a specific URL, call Javascript code, and even include a monitor-specific CGI request to an external resource. At present, only one custom column is support in SiteScope.

Custom columns can be created without creating a custom property. For example, You can create a custom column to display a fixed hyperlink to an external resource in the SiteScope interface. You can display custom monitor properties in a custom column. For details, see “Displaying Custom Properties in Custom Columns” on page 1375.

You can also embed short Javascript code into a custom column. A script can call other custom scripts that you can add or reference by using the headerHTML parameter in the master.config file. For example, you can write a script as an external file called sscopecustom.js in the **<install_path>\SiteScope\** folder and then reference this file by adding the following to the headerHTML entry:

```
_headerHTML=<script language=”Javascript” src=”sscopecustom.js”></script>
```

Note: When adding Javascript using the headerHTML parameter, use the existing entry in the master.config. Only one headerHTML parameter is allowed.

Custom Column Definition Syntax

You define a custom column definition using the following syntax:

_monitorTableCustom=_*referenceValue*|*column_title*|*column_content_definition*

The custom elements of the definition string are separated by the vertical pipe (|) symbol. The following table describes the elements of the custom property definition string.

Element	Description
_monitorEditCustom	The parameter name that signals SiteScope to add a custom monitor property to monitors.
_referenceValue	The variable name for the property. Generally, this is a placeholder name although it can be referenced in other places within SiteScope.
column_title	The text to display as the column title.
column_content_definition	The text string or markup code to be displayed in the custom column for each monitor. This can include HTML and Javascript code.

Note: The entire definition string must be on a single line of text. Do not insert any linefeeds or carriage returns in the column definition.

You use the following steps to add a custom column to the SiteScope real-time views.

To add a custom column:

1. Make a backup of the master configuration file in a safe location. The file is found at **<install_path>\SiteScope\groups\master.config** on the machine where SiteScope is running.
2. Open **master.config** using a text editor.
3. Add a _monitorTableCustom= entry as a new line to the file.
4. On the same line, enter the text string to define the _referenceValue, the column_title and the column_content_definition. Separate each of the entries with the vertical pipe (|) symbol.
5. Save the changes to the file.

Displaying Custom Properties in Custom Columns

By default, custom monitor properties are displayed only in the Properties view of an individual monitor. This means that they are not normally visible in real-time views. In some cases, a custom monitor property is useful only if the value is displayed in the interface. You can display custom properties in Dashboard views by adding a reference to the property in a custom column.

The following is an overview of the steps you use to link monitor properties to custom columns:

1. Create a custom property definition.
2. Create a custom column definition.
3. Reference the custom property variable in the custom column definition.

Referencing Monitor Properties in Custom Columns

When you define a custom monitor property, SiteScope adds the name of the property to its list of properties for the monitor. You can display these properties in custom columns by adding a reference to one or more property variables in the column content definition string. Use the following steps to add references to custom properties to the content definition for custom columns.

To reference property values in custom columns:

1. Make a backup of the master configuration file in a safe location. The file is found at <install_path>\SiteScope\groups\master.config on the machine where SiteScope is running.
2. Open **master.config** using a text editor.
3. Add one or more _monitorEditCustom= entries including the *_propertyName*, the *display_title* and the *display_description* strings. Separate each of the entries with the vertical pipe (|) symbol.
4. Add a _monitorEditCustom= entry including the _referenceValue, the column_title and the column_content_definition. Separate each of the entries with the vertical pipe (|) symbol.

5 Within the string for the column_content_definition, include a reference to a custom property by adding the _propertyName surrounded with dollar signs ($). For example, if a custom property is defined with the name _NOCAction, add a reference to this property in the column_content_definition as $_NOCAction$.

6 Save the changes to the file.

You may include references to some other internal SiteScope property variables in the column_content_definition string. This is limited to property variables specific to each monitor type.

82

Tools for Troubleshooting

When SiteScope reports a problem with a monitored system or you are having difficulty configuring a monitor, it is useful to have some resources to troubleshoot and diagnose problems. SiteScope provides a number of tools to help you uncover issues and facilitate monitor configuration.

About SiteScope Tools

The SiteScope Tools node contains a number of utilities that are useful to test the monitoring environment. Use these tools to make a variety of requests and queries of systems you are monitoring and to view detailed results of the action. Requests may include simply testing network connectivity or verifying login authentication for accessing an external database or service.

The following tables list the diagnostic tools that are available. See the applicable sections for more information about these tools.

Application Diagnostic Tools

Tool Name	Description
DNS Lookup	Test a DNS server to verify that it can resolve a domain name. (Includes access to a Traceroute tool to test network routing.).
Database Connection	Check connectivity and configuration of JDBC or ODBC database connections.
Database Information	Retrieve and display database server metadata such as product and driver version, SQL compatibility level information, and supported SQL functions.
FTP Server	Check the availability of an FTP server and whether a file can be retrieved.
Get URL and URL Content	Request a URL from a server and prints the returned data. Includes access to a Trace Route tool to test network routing.
Mail Round Trip Test	Test a mail server by sending and retrieving a test message.
Ping	Perform a round-trip Ping test across the network. Includes access to a Traceroute tool to test network routing.
Trace Route	Perform a traceroute from your server to another location.
SNMP Browser	Browse an SNMP MIB and view available OIDs.
SNMP	Performs a SNMP get command to a specified SNMP host to retrieve a list of OIDs.
SNMP Trap	View the log of SNMP Traps received by SiteScope from SNMP-enabled devices.
Check URL Sequence	Retrieve a sequence of URLs.
Web Service	Test the availability of SOAP enabled Web Services.
XSL Transform Test	Test custom XSL transformation of XML data to be monitored with the Browsable XML Monitor.

Server Diagnostic Tools

Tool Name	Description
Network	Display the server's network interface status and active connections.
Processes	Show a list of currently running processes either locally or on a remote server.
Services	Show a list of currently running Windows Services.

Advanced Diagnostic Tools

Tool Name	Description
News Server	Check whether a News Server is operational.
Event Log	Display portions of the Windows Event Log locally or on a remote server.
LDAP Authentication	Test an LDAP server by requesting a user authentication.
Performance Counters	Check connectivity to and values in Win NT Performance Counter registries.
Regular Expression	Test a regular expression for content matching against a sample of the content you want to monitor.

Working with SiteScope Tools

You access the SiteScope Tools by expanding the Tools node in the left menu tree and then clicking on the icon or name for the tool you want to use. The tool form is displayed in the Contents area.

The following sections describe how to use each of the SiteScope diagnostic tools.

Database Connection

The Database Connection diagnostic tool is used to test and verify connectivity between SiteScope and an external ODBC or JDBC compatible database. This diagnostic tool checks to see if:

- the supplied database driver can be found and loaded
- a connection can be made to the database
- an optional SQL query can be executed and the results displayed
- the database connection and resources can be closed

If exceptions or errors occur during the test, the information is printed along with suggested actions to help with troubleshooting. This tool can be useful in verifying connection parameter values needed to set up database monitors, database alerts, and database logging.

Database Connection URL

Enter the connection URL to the database you want to connect to. The syntax is jdbc:oracle:thin:@<server name or ip address>:<database server port>:<sid>.

For example, to connect to the ORCL database on a machine using port 1521, use:

```
jdbc:oracle:thin:@206.168.191.19:1521:ORCL.
```

The colon (:) and @ symbols must be included as shown.

Note: If you want to access the database using Windows authentication, enter jdbc:mercury:sqlserver://<server name or IP address>:1433 DatabaseName=<database name>;AuthenticationMethod=type2 as the connection URL, and com.mercury.jdbc.sqlserver.SQLServerDriver as your database driver. Leave the **Database User Name** and **Database Password** boxes empty so that the credentials of the currently logged on Windows user (the account from which SiteScope service is running) are used to establish a connection to the database.

Database Driver

Enter the JDBC or ODBC driver that SiteScope should use. The **.jar** file or library containing the **.class** file must be installed in the <**SiteScope install path**>**\SiteScope\java\lib\ext** directory. To use a database other than jdbc:odbc:orders, you must install the driver files into the proper directory before SiteScope can use them.

Database User Name

Enter the user name required to connect to the database.

Database Password

Enter the password required to connect to the database.

Query

(Optional) Enter a SQL query to execute on the database. If you do not supply an SQL query string, the driver is loaded and the connection to the database is tested but no query is executed.

Results Set Max Columns

If you have entered a SQL Query, enter the maximum number of columns to display in the query result set.

Results Set Max Rows

If you have entered a SQL Query, enter the maximum number of rows to display in the query result set.

Click the **Connect and Execute Query** button to run the connection test. Connection results are shown beneath the button.

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

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

Database Information

The Database Information diagnostic tool is used to display database server metadata such as product and driver version, SQL compatibility level information, and supported SQL functions.

Database Connection URL

Enter the connection URL to the database you want to connect to. The syntax is jdbc:oracle:thin:@<server name or ip address>:<database server port>:<sid>.

For example, to connect to the ORCL database on a machine using port 1521, use:

```
jdbc:oracle:thin:@206.168.191.19:1521:ORCL.
```

Note: The colon (:) and @ symbols must be included as shown.

Database Driver

Enter the JDBC or ODBC driver that SiteScope should use. The **.jar** file or library containing the **.class** file must be installed in the **<SiteScope install path>\SiteScope\java\lib\ext** directory. To use a database other than jdbc:odbc:orders, you must install the driver files into the proper directory before SiteScope can use them.

Database User Name

Enter the user name required to connect to the database.

Database Password

Enter the password required to connect to the database.

Click the **Get Database Info** button to display database information. Connection results are shown beneath the button.

Note: Different drivers and user names can significantly change what information is displayed.

DNS Lookup

DNS Lookup is a tool which looks up names from a Domain Name Server and shows you the IP address for a domain name. It also shows you information about the name servers for a domain.

When there is a problem on the network, one cause may be that the DNS server is not providing the right IP addresses for your servers. You can use this utility to verify that your DNS server is returning the correct addresses for your own servers. You can also use it to verify that it is able to look up the addresses for external domains.

The DNS Lookup form provides a gateway to the standard nslookup program. It sends the request to the DNS server entered in the DNS Address text box and displays the IP address for the host name entered in the Host Name text box.

Click the **DNS Lookup** button to initiate the test. The results of DNS Lookup are displayed below the button.

Event Log

The Windows NT Event Log tool displays event log entries on a server. By default, the Event Log tool displays entries from the System log for the server on which SiteScope is installed. The log entries are displayed below the **Show Event Log Entries** button. You can view the entries in the event logs on another server by entering the name of that server in the **Server Name** text box. You use the drop-down list in the **Event Log** box to choose which type of log file to view. The choices include the following:

- System
- Application
- Security

You use the **Entries To Show** box to specify how many entries from the log file you want displayed. The ten most recent entries are shown by default with the latest entry always displayed at the bottom of the list.

Clicking the **Show Event Log Entries** button completes the action and refreshes the log entry listing.

FTP Server

You can use the Check FTP Server tool to access an FTP server and view the interaction between SiteScope (acting as an FTP client) and the FTP server. For example, if you receive an alert from SiteScope indicating that your FTP server is not working properly, the first step is to use this tool to help track down the problem.

To check an FTP server Complete the items on the Check FTP Server form as outlined below. When the required items are complete, click the **Check FTP Server** button to initiate the test.

FTP Server

Enter the IP address or the name of the FTP server that you want to test. For example, you could enter either 206.168.191.22 or ftp.thiscompany.com.

File

Enter the file name to retrieve (for example, /pub/docs/mydoc.txt).

User Name

Enter the name used to log into the FTP server.

Password

Enter the password used to log into the FTP server.

Use Passive

Select this check box to have SiteScope use a passive FTP connection. This is commonly required to access FTP servers through a firewall.

Proxy

Enter the proxy name or IP address if you want to use a proxy server for the FTP test.

Proxy User Name

Enter the name used to log into the proxy server.

Proxy User Password

Enter the password used to log into the proxy server.

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

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

Get URL and URL Content

Use the Get URL and URL Content tool to retrieve an item from a Web server. The URL specifies the server to contact and the item to return. Because SiteScope displays the content of the requested URL, this tool also functions to check URL Content. You can use this utility to verify that a given URL can be accessed from a Web server. You can also use it to see how long it takes for the page to be returned.

Click the **Get URL** button to initiate the test. Complete the Get URL form as indicated. The results of the test are displayed on the lower portion of the page. The results include statistics on the URL retrieval as well as a text representation of the URL content.

URL

Enter the URL that you want to test (for example, http://demo.company.com).

URL Content Encoding

Encoding compresses the content before it is sent to the client. The content is decoded by the client. An example of encoding is ISO8859-1.

If you use more than one encoding, they must be separated by commas (,) and in the exact order in which they are to be performed on the URL content.

User Name

If the URL specified above requires a name and password for access, enter the user name.

Password

If the URL specified requires a name and password for access, enter the password.

Domain (only on Windows platform)

Enter the domain name of the SiteScope server.

Use NTLM V2

Check this parameter if you want to use NTLM (Windows NT LAN Manager) version 2 to authenticate user logon.

Proxy

Optionally, a proxy server can be used to access the URL. Enter the address or domain name and port of an HTTP Proxy Server.

Proxy User Name / Proxy Password

Enter the user name and password to proxy server to access the URL.

Proxy Use NTLM V2

Check this parameter if the proxy uses NTLM (Windows NT LAN Manager) version 2 to authenticate user logon.

Content Match

Enter a string of text to check for in the returned page or frame set. If the text is not contained in the page, the content match fails. The search is case sensitive. HTML tags are part of a text document, so you must include the HTML tags if they are part of the text you are searching for (for example, "< B> Hello< /B> World").

Error Content Match

Enter a string of text to check for in the returned page or frame set. If the text is contained in the page, the test indicates an error condition. The search is case sensitive.

Retrieve Frames

Check this option to have SiteScope display the HTML code of a frame linked to the URL being requested.

Retrieve Images

Check this option to have SiteScope list the images such as graphics, logos, and so on linked to the URL being requested.

LDAP Authentication

The SiteScope LDAP Authentication Test verifies that a Lightweight Directory Access Protocol (LDAP) server can authenticate a user by performing a simple authentication.

Complete the items on the LDAP Authentication Test form and then click **Authenticate User**.

Security Principal

Enter the constant that holds the name of the environment property for specifying the identity of the principal that authenticates the caller to the service. The format of the principal depends on the authentication scheme. If this property is unspecified, the behavior is determined by the service provider. This should in the format: uid=testuser,ou=TEST,o=mydomain.com.

Note: Users may be defined with special characters in your LDAP server. However SiteScope does not support users that contains one or more of the following character inside the users name: equal ("="), semi-colon (";"), inverted commas (""").

Security Credential

Enter the constant that holds the name of the environment property for specifying the credentials of the principal for authenticating the caller to the service. The value of the property depends on the authentication scheme. For example, it could be a hashed password, clear-text password, key, certificate, and so on. If this property is unspecified, the behavior is determined by the service provider.

URL Provider Address

Enter the constant that holds the name of the environment property for specifying configuration information for the service provider to use. The value of the property should contain a URL string (for example, ldap://<somehost>:389). 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.

LDAP Query

Use this box to enter an object query to look at a LDAP object other than the default user **dn** object. For example, enter the mail object to check for an e-mail 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. For details about the search filter, see the description below.

Search Filter

Enter an search filter in this text box to perform a search using a filter criteria. The LDAP filter syntax is a logical expression in prefix notation meaning that logical operator appears before its arguments. For example, the item sn=Freddie means that the **sn** attribute must exist with the attribute value equal to Freddie.

Multiple items can be included in the filter string by enclosing them in parentheses, such as (sn=Freddie) and combined using logical operators such as the & (the conjunction operator) to create logical expressions. For example, the filter syntax (& (sn=Freddie) (mail=*)) requests LDAP entries that have both a sn attribute of Freddie and a mail attribute.

More information about LDAP filter syntax can be found at http://www.ietf.org/rfc/rfc2254.txt and at http://java.sun.com/products/jndi/tutorial/basics/directory/filter.html.

Mail Round Trip Test

The SiteScope Mail Test checks a Mail Server via the network. It verifies 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 via a POP user account. Each message that SiteScope sends includes a unique key which it checks for to insure that it does not retrieve the wrong message and return a false OK reading.

Complete the items on the Mail Monitor form as follows. When all the fields are complete, click the **Check Mail Server** button.

Message

Select the action to take:

- **Send & Receive.** This option allows you to send a test message to an SMTP server and then receive it back from the POP3 or IMAP4 server to check that the mail server is up and running.
- **Receive Only.** This option checks the incoming POP3 or IMAP4 mail servers for a message that was sent previously. This check is done by matching the content of the previously-sent message.

Note: If the **Receive Only** option is selected, the Content Match text box must have a value to match against.

- **Send Only.** This option checks that the receiving mail server has accepted the message.

Send To Address

Enter the mail address to which the test message should be sent. This should be the address for the POP account that you specified in the **Mail Server User Name** box. For example, if you specified support as the Mail Server User Name, the Send To Address might be support@mycompany.com.

Sending Mail Server (SMTP)

Enter the hostname of the SMTP mail server to which the test mail message should be sent (for example, mail.thiscompany.com).

Receiving Server Type

Select the protocol used by the receiving mail server. Use the POP3 option to check the POP3 mail server for a sent message. Use the IMAP4 option to check the IMAP mail server for a sent message.

Receiving Mail Server

Enter the hostname of the POP mail server that should receive the test message. This can be the same mail server to which the test message was sent (for example, mail.thiscompany.com).

Receiving Mail Server User Name

Enter a POP user account name. A test e-mail message is sent to this account and the Mail monitor logs in to the account to verify that the message was received. No other mail in the account is touched. You can use your own personal mail account or another existing account for this purpose.

Note: If you use an e-mail reader that automatically retrieves and deletes messages from the server, there is a chance that the Mail Monitor never sees the mail message and reports an error.

Receiving Mail Server Password

Enter a password, if necessary, for the test mail account.

NTLM Authentication

If NTLM authentication is used by the e-mail server, choose if you need version 1 or version 2.

Timeout

The number of seconds to wait for a mail message to be received before timing-out. The default is 300 seconds.

Retrieve Pause

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.

Content Match

Enter a string of text to match against the contents of the incoming message. If the text is not contained in the incoming message, the monitor is in error. This is for the receiving only option (for example, Subject:MySubject). The search is case sensitive.

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, "< B> Hello< /B> World"). This works for XML pages as well.

You can perform a regular expression match by enclosing the string in forward slashes, with an i after the trailing slash indicating case-insensitive matching. An example might be "/href=Doc\d+\.html/" or "/href=doc\d+\.html/i".

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+)/). This returns the temperature as it appears on the page and can be used when setting an Error if or Warning if threshold.

Show Details

Select this box if you want details of the round trip test to be displayed.

Network

The Network Tool reports the current network interface statistics and lists the active network connections. This information can be useful to determine the health of you network interface. You can also use this tool to track down problems where network connections are being left open or runaway conditions where more and more connections are being opened without ever being closed.

The Network Tool runs once when it is opened and reports the network information. The data returned by the tool are displayed on the lower portion of the Network Tool page. The information can be updated by clicking on the **Run Network** button.

News Server

You can use the Check News Server as a tool to access a news server and view the NNTP interaction between SiteScope (acting as a news client) and the news server.

To perform a news server check, complete the Check News Server form as indicated. You can optionally specify one or more news groups by entering them into the **News group** text box. Separate multiple news group names by commas. If the news server requires a user name and password, enter them in the boxes provided. Clicking the **Check News Group** button initiates the test. The results of the test is displayed in the lower portion of the page.

Ping

Ping is a tool that sends a packet to another location and back to the sender. It shows you the round-trip time along the path. When there is a problem with the network, ping can tell you if another location can be reached. The Ping tool does a ping from the current server to another location. Enter the domain name or IP address of the location you want to ping in the text box.

For example, enter either:

```
demo.thiscompany.com (this is the host name)
```

or

```
206.168.112.53 (this is the host’s IP address)
```

Output similar to the following is displayed on the screen:

```
Pinging 206.168.112.53 with 32 bytes of data:
Reply from 206.168.112.53: bytes=32 time=20ms TTL=59
Reply from 206.168.112.53: bytes=32 time=10ms TTL=59
Reply from 206.168.112.53: bytes=32 time=10ms TTL=59
Reply from 206.168.112.53: bytes=32 time=10ms TTL=59
Reply from 206.168.112.53: bytes=32 time=20ms TTL=59
```

Performance Counters

The Performance Counter Test is a tool that you can use to check performance counters on a specific machine in an Windows NT/2000 network. It provides is an interface to the perfex.exe executable supplied as part of SiteScope.

Complete the form as shown and click the **List Objects and Enumerate Counters** button to display the individual performance counters and the corresponding values for the selected counter object. If there are no counter objects available for this machine, the drop-down list that contains the counter objects indicates this situation. Information about the problem is shown along with suggested actions to resolve the problem. This tool can be very useful in troubleshooting remote registry connections needed to read performance counters.

Machine Name

Enter a machine name to list all NT performance counter objects available on that machine. A double slash ,\\, is automatically prefixed to any machine name supplied. If this box is left blank, the default is the local machine (**this server**).

Admin User Account / Password

Enter the administrative user name and password for the machine you want to query. This is only necessary if you running SiteScope under an account that does not have administrative privileges to access performance counters for the domain or workgroup you are trying to connect to.

If the test indicates you are required to supply a password, it means that the remote machine requires authorization to access the performance counter registry.

Counter Object Name

Use the drop-down list to select the counters to list. This box displays one of the following values:

- **Choose a counter object.** Choose a counter object from the drop-down list. Click the **List Objects and Enumerate Counters** button to display the individual NT performance counters and corresponding values for the selected counter object.
- **NO COUNTER OBJECTS AVAILABLE using this user name and password**. You must provide a user name and password to see the counter objects. The remote machine you are connecting to does not recognize the user that the SiteScope service is currently running as **VALID user with local admin rights**. If you believe you have the correct user name and password, click the **List Objects and Enumerate Counters** button to update the display.
- **<One of the counter objects available on the machine named in the Machine Name box>**. A counter selection has already been made.

The data for that counter is displayed in the table in the lower portion of the page. The table shows the counter name, the value, and a description of the counter provided by the counter registry:

Counter Name	Counter Value	Counter Description

Other troubleshooting tips are available on the NT Performance Counter Test page.

Processes

The Processes tool displays processes running on the server where SiteScope is installed. This can be useful to confirm that critical processes are available. If Remote UNIX machines have been defined, they are listed in a drop-down menu.

You can view processes running on a machine by entering the name of the Remote UNIX server or the server where SiteScope is installed in the **Server Name** text box. Click **Show Processes**.

Regular Expression

Cut and paste a portion of text on which you want to perform a regular expression match into the text box labeled **Your Text that will be matched**. For efficiency in developing regular expressions, you should include all of the content that would precede the target data or pattern that you want to match. For example, when developing a regular expression for content matching on a Web page, you should use the Get URL and URL Content tool to retrieve the entire HTTP content including the HTTP header.

You enter your test regular expression into the field labeled **Your Regular Expression**. For content with multiple lines with carriage returns and line feeds, consider adding the `s` search modifier to the end of the expression to have the content treated as a single line of text (for example, `/value:\W[\d]{2,6}/s`). Click the **Test Your Match** button to perform the match test.

The results of the test are displayed in the area below the **Test Your Match** button. If there is a problem with your regular expression, an error message is displayed.

Parsed parentheses and matches

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

- **Parentheses counted from left.** This displays any patterns in the regular expression delimited by parentheses as counted from the left-hand side of the expression.
- **Matching text.** This table cell displays the text that matched the parenthesis marked patterns listed in the column to the left.

Below this table is the **Whole Match Between Slashes** text area. This echoes the entire content entered in the **Your Text that will be matched** field. The content that matched the pattern in your regular expression is highlighted within this content, normally using a blue font. This can be very useful to show possible problems with wildcard expressions like the .* pattern that match too much content. It can also uncover problems of duplicate patterns within the content that require you to add other unique patterns to your expression to match the desired portion of the content.

SNMP Browser

The SNMP Browser Tool provides a browsable tree representation of an SNMP agent's MIB. It can be used to verify the connection properties of an SNMP agent and to gain more information about the MIBs which that agent implements.

This tool operates by traversing all of the OIDs on a given agent and then using the MIB information in the <SiteScope root directory>/templates.mib directory to build a tree-structured XML representation of the OIDs. Included in the XML tree are the textual and numeric names of the OIDs, their descriptions (if available), and their values at the time of traversal.

The XML is displayed in a separate browser window, using the browser's default display for XML data. For IE and Netscape/Mozilla browsers, this default display is in the form of a collapsible, hierarchical tree. If errors occur during the MIB traversal, then an error message describing the problem is printed in the new window (instead of XML).

The SNMP by MIB Tool is intended to help in configuring any of the SNMP-based monitors, including:

- SNMP by MIB Monitor
- SNMP Monitor
- Cisco Works Monitor
- F5 SNMP Monitor

Complete the tool form as shown and click the **Browse** button to open a new window containing a browsable view of the MIB (in XML).

Host or IP Address

Enter the hostname or IP address of the device on which the SNMP agent is running.

Port

Enter the port on which the SNMP agent is listening. This is usually 161, which is also the default.

MIB

Choose the MIB that you want to view. If you select **All MIBs**, then all data obtained during the MIB traversal is displayed. If you select a specific MIB, then only the OIDs within that MIB are displayed. This list of MIBs can be updated or extended by placing new MIB files in the **<SiteScope root directory>/templates.mib** directory.

Starting OID

Use this option when selecting counters for this monitor. When the monitor attempts to retrieve the SNMP agent's tree, it starts with the OID value that is entered in this field. The default value is 1, which is commonly used and applicable to most applications. You should edit this field 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 in this field.

Version

Select the version of SNMP which the tool should use when connecting to the agent.

V1/V2 Community

For version 1 or 2 connections, enter the community string to use when connecting to the SNMP agent.

V3 Authentication Type

Select the type of authentication to use for a version 3 connection.

V3 Username

Enter the user name for a version 3 connection.

V3 Authentication Password

Enter the password to use for authentication in a version 3 connection.

V3 Privacy Password

Enter the password to use for DES privacy encryption in a version 3 connection. Leave this field blank if no privacy is desired.

V3 Context Engine ID

Enter a hexidecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.

V3 Context Name

Enter the Context Name to use for this connection. This is applicable for SNMP V3 only.

SNMP

The SNMP tool lets you query a SNMP Management Information Base (MIB) and retrieve a set of OIDs. Fill out the SNMP tool form as shown below then click the **Next Block of OIDs** button to perform the query (GET).

Host IP Address

Enter the IP Address of the server that hosts the SNMP MIB you want to query.

By default, SNMP connects to port 161. If your SNMP device uses a different port, append the port number to the host name. For example, to use port 170, type demo.sitescope.com:170.

Next OID

Enter the OID of the next OID that should be retrieved.

Index

Enter the index of the SNMP object. Values for an OID come as either scalar or indexed (array) values. For a scalar OID, the index value must be set to 0. For an indexed value, you must provide the index (a positive integer starting with 1) to the element that contains the value you want. For example, the OID 1.3.6.1.2.1.2.2.1.17 is an indexed value that contains four elements. To access this second element of this OID you enter an index of 2 in this text box.

Community

Enter the Community string for the SNMP device. Most devices use "public" as a community string. If the device you are testing requires a different Community string, supply it in this box.

Version (V1 or V2)

Select the SNMP version used by the SNMP host you want to test. SiteScope supports both SNMP version 1 and version 2.

Number of Records to get

Enter the number of OID records to retrieve.

The SNMP OIDs returned by the SNMP Tool are displayed in the lower portion of the page.

SNMP Trap

The SNMP Trap log tool lets you view SNMP Trap received by SiteScope's SNMP listener. The tool is only enabled if you have already created one or more SNMP Trap Monitors. Creating an SNMP Trap Monitor enables the SiteScope SNMP Trap Log. The message **Receiving SNMP Traps is not active** is displayed at the top of the tool page if the SNMP Trap Log is not currently active.

Fill out the SNMP Trap log tool form as shown below then click the **Show SNMP Trap Log Entries** to view the log based on the search criteria you have entered.

Traps To Show

Enter the number of SNMP Traps to list. The default is 10. The most recent SNMP Traps received by SiteScope are displayed first.

Content Match

Enter an optional text string or regular expression to be used to match entries in the SNMP Trap Log. Content matching can be done for data from any of the columns of the log such as OID, Community, Agent, and so on.

The SNMP traps in the SiteScope SNMP Trap Log are displayed in the SNMP Trap Log table. The number of traps matching the search criteria are displayed in the table title. The format of the table is as follows:

SNMP Trap Log (0 traps)

Date	From	Message	Trap	Specific	OID	Agent	Community	Trap Time

Services

The Services tool displays services running on the server where SiteScope is installed. This can be useful to confirm that critical services are available. If Remote UNIX machines have been defined, they are listed in a drop-down menu.

You can view services running on a machine by entering the name of the Remote UNIX server or the server where SiteScope is installed in the **Server Name** text box. Click **Show Services**.

Trace Route

Trace Route is a tool that shows you the network path between two locations and how long it takes to get to each hop in the path. When there is a problem with the network, traceroute can often be used to narrow down where the problem is occurring. This tool performs a traceroute from your server to another location. The Trace Route tool is accessible by a link below the navigation bar on the Ping, the Get URL, and DNS Lookup tool pages.

The Trace Route form provides a gateway to the standard traceroute program which determines the route across a network taken by packets from one host to another host. In this case, the traceroute starts from your server. It displays the path taken to reach the host or IP address you have listed in the text box.

You can use this utility to verify connectivity of a host and to determine how the host is connected to the Internet. You can also determine the path taken from your server to the specified host. This helps you to determine where packet loss may be occurring when you attempt to connect to hosts elsewhere on the Internet.

To perform a traceroute on Windows:

1. Enter the domain name or IP address of the other location in the text box.
2. Click **Trace Route** to initiate the action.

Note: For SiteScope on UNIX platforms, specify the path name to the traceroute utility on the server that SiteScope is running on.

To perform a traceroute on UNIX:

1. Stop the SiteScope process.
2. In the left menu tree, expand **Preferences** and choose **Infrastructure Settings Preferences**. The General Settings view opens.
3. Click **Edit.** The Edit Infrastructure Settings Preferences window opens.
4. In the **Traceroute command** box, add the path of the traceroute utility. For example:

   ```
   /usr/sbin/traceroute
   ```
5. Click **OK** to save your changes.
6. Restart the SiteScope process.

Check URL Sequence

The Check URL Sequence Tool simulates a user's session across several pages. An example of this would be entering an account name via a Web form, checking an account status for the page that is returned, and then following a sequence of links through several more pages.

The Check URL Sequence Tool page is accessed either by clicking the **Tools** link that is displayed with the monitor status in the Monitor Detail table or by clicking the **Check URL Sequence** link on the Diagnostic Tools page.

Note: Accessing the Check URL Sequence Tool via the Monitor Detail page is considered to be more useful than using it as a diagnostic tool. Access via the Monitor Detail page allows you to modify existing URL Sequences including use of the URL Sequence Wizard.

A URL Sequence is specified by giving a URL to start at and then specifying either additional URLs, or more commonly, links or buttons to follow. For each step you may specify a match or error string to search for, a user name and password to enter, and POST data for that step.

The URL Sequence tool returns the status and time taken for each step in the sequence. It also embeds a copy of the page returned at each step of the sequence in it is output so that a more graphical view of the sequence can be viewed.

Complete the items on the Check URL Sequence form as follows. When the required items are complete, click the **Check URL Sequence** button to test the transaction or the **Update Monitor** button to save any changes that you have made to the current monitor. Press the **Press the Wizard** button to edit the existing sequence in the URL Sequence Wizard interface.

Step 1 - Reference

Select the type of object or target from the drop-down list in the first column. This represents the either a Web page, a hyper link, form element, and so on, that defines the sequence path. The type for Step 1 should always be a URL. Enter the specific URL of the first page in the sequence that you want SiteScope to complete.

For example, if you want SiteScope to test your order process, you might enter a URL such as https://www.securecompany.com/order.html.

Step (2 thru N) - Reference

From Step 2 on, you must tell SiteScope what you want it to do next. In the Type column, tell SiteScope what type of item to look for in this step. For example, if SiteScope is to do the equivalent of selecting a submit button, you would choose the **Form - match the displayed name of a Submit button**. SiteScope uses this information to scan the HTML for the proper text matches.

Enter the URL, link, or Submit button to be followed in the second column for this step. For example, if SiteScope should follow the Submit button on the page and the name on the button (its value) is Place My Order, type Place My Order in this text box. To instruct SiteScope to follow a link on the page, type the text of the link. For example, if the link says Next, type the word Next in this text box. You can also type in a full URL.

If an image is used as the Submit button, you must enter the name value for the image. You find this name value by looking at the HTML for the form.

The Advanced Settings section gives you the ability to customize error and warning thresholds, or complete other optional settings.

POST Data

If this step contains a URL 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. See also the Match Content box for a way to verify that the correct form response was received. If this item is blank, a GET request is performed.

Match Content

Enter an expression describing the values to match in the returned page. If the expression is not contained in the page, the message **no match on content** is displayed. A regular expression can be used to define the values to match.

Error If Match

Enter an expression describing the values that, if found on the page returned, indicate an error in the sequence process. For example, if the phrase **Login Error** appears, there may be a problem with user profile data. If the **Error If Match** expression is found in the page, the monitor signals an error. A regular expression can be used to define the values to match.

User Name

Enter the user name, if any, required for this step.

Password

Enter the password, if any, required for this step.

Delay

Enter an optional delay period that SiteScope waits before executing the next step.

Title

Enter an optional title to be associated with this step of the sequence. It is best to select a title that describes what is being accomplished in this step.

Web Service

The Web Service Test is used to check Simple Object Access Protocol (SOAP) enabled Web services for availability, stability, or to see what an actual SOAP response looks like. It is also useful for diagnosing a Web service request failure, or for picking out match strings for use with a specific Web Service Monitor. The Web Service Test sends a SOAP request to the server and checks the HTTP response codes to verify that the service is responding. The actual SOAP response is displayed, but no further verification is done on this returned message.

The Simple Object Access Protocol (SOAP) is a way for a program running under one operating system to communicate with another program running under the same or different operating system (such as a Windows 2000 program talking to a Linux-based program). SOAP uses the Hypertext Transfer Protocol (HTTP) and Extensible Markup Language (XML) for information exchange with services in a distributed environment.

Status

The possible status values returned by the test 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

Support Levels

The following specification features are currently supported:

- WSDL 1.2
- SOAP 1.1
- Simple and Complex Types based on XML Schema 2001
- SOAP binding with the HTTP(s) protocol only
- SOAP with Attachments is not supported

Important: 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.

Tip: A quick way to fill out this form is to first create a Web service monitor for the service you need to test. In the **Add Web Service Monitor** page, specify the WSDL file of the target Web service. SiteScope parses the WSDL file, presents a list of methods to choose from, and then generates a skeleton parameter list for your selected method. Save and create this Web service. SiteScope sends the proper SOAP message to invoke the service method (that may or may not succeed). Once the Web service monitor is created, it is listed in your Group monitors display page. Clicking the **Tools** link for this Web service monitor returns you to the **Test Web Service** page with the test form properly completed.

As an alternative, manually complete the items on the **Add Web Service Test** form as follows. When the required items are complete, click the **Web Service Request** button.

WSDL Path or URL

Enter the URL or the file path of the WSDL file to be used for this monitor. If a WSDL file path is specified it must be relative to **<SiteScope install path>/SiteScope/templates.wsdl/**. In addition, your WSDL files must have an extension of .wsdl.

Web Service URL

Enter the URL of the Web service to be tested.

Method Name

Enter the name of the method to be invoked.

Arguments

Enter the arguments to the method specified above and their types. Specify simple type parameters in the format
parm-name(parm-type) = value.

where the <param-name> and <param-type> must match the service method specifications of its WSDL file exactly. The <value> must agree with the <param-type>, otherwise the request fails. Strings with embedded spaces should be enclosed in double quotes (" "). Each parameter must be on a separate line by adding a carriage return at the end of each value.

For example:

```
stockSymbol (string) = MERQ
numShares (int) = 10
```

A complex type parameter must be represented as one long string. An example of a complex type parameter is shown (line breaks are for readability purposes only):

```
stocksymbol[COMPLEX] =
<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">
<ticker xsi:type="xsd:string">MERQ
</ticker>
</stocksymbol>
```

SiteScope does not perform any validation on your input parameter lists, so make sure that the complex type values are valid and well-formed XML strings. Do not add any carriage returns within a complex type parameter - only at the end.

If the Web service method does not take any parameters, the text box should be left empty.

SOAP Action URI

The SOAP Action URI in the header of the SOAP request to the Web Service. During initial setup this is extracted from the WSDL file.

User-Agent

Enter the user agent that sends the request (Mozilla, Internet Explorer, and so on).

Method Namespace

The XML name space for the method in the SOAP request. During initial setup this value is extracted from the WSDL file.

User Name

If the URL specified requires a name and password for access, enter the name.

Password

If the URL specified requires a name and password for access, enter the password.

NTLM Domain

Enter the domain for NT LAN Manager (NTLM) authorization if it is required to access the URL.

Proxy

Optionally, a proxy server can be used to access the URL. Enter the domain name and port of the HTTP Proxy Server.

Proxy User / Proxy Password

If the proxy server requires a name and password to access the URL, enter the user name. Your proxy server must support Proxy-Authenticate for this options to function.

XSL Transform Test

Use this tool to test a user defined XSL file that can be used to transform an XML file or output. This might be a file from a Web application that contains performance metrics data. The use of an XSL transform may be necessary to process the XML data into an acceptable format for use by the Browsable XML Monitor type. The format rules for said input XML are:

XML URL

Enter the URL of the XML file that is the input for the transformation.

XSL File

Enter the path to the XSL file you want to test.

User Name

If access to the target XML file requires authentication, enter the user name needed to access the content.

Password

If access to the target XML file requires authentication, enter the password needed to access the content.

Proxy

If you are using a proxy to access the target XML content, enter the address of the proxy.

Proxy User Name / Proxy Password

If you are using a proxy to access the target XML content, enter the user name needed to use the proxy in this field.

Index