HP SiteScope

for the Windows, Solaris, and Linux operating systems

Software Version: 11.10

Using SiteScope

Document Release Date: February 2011
Software Release Date: February 2011

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

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

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

iPod is a trademark of Apple Computer, Inc.

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

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

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

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation (**http://www.apache.org/**).

This product includes software developed by the JDOM Project (**http://www.jdom.org/**).

Documentation Updates

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

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

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

http://h20230.www2.hp.com/selfsolve/manuals

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

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

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

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

Support

Visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Table of Contents

PART III: INTEGRATIONS

PART IV: MONITORS

PART V: INTEGRATION MONITORS

Welcome to This Guide

This guide describes how to configure and use HP SiteScope's agentless monitoring solution to monitor the availability and performance of your distributed IT infrastructure.

This chapter includes:

How This Guide Is Organized

The guide contains the following parts:

Part I Introduction to SiteScope

Introduces SiteScope and provides an overview of the SiteScope key features and the monitoring model.

Part II General and Administration

Describes how to set up and administer SiteScope, access SiteScope, use silent login, SiteScope configuration API, SiteScope iPhone application, integrate SiteScope with other products, and provides a working order for using SiteScope.

It also describes how to navigate the SiteScope user interface, search and filter SiteScope objects, use Global Search and Replace, use SiteScope tools to troubleshoot resource and monitor configuration problems, and use regular expressions.

Part III Integrations

Describes how to use SiteScope to send metrics and report topology data to HP Business Service Management (BSM), how to use SiteScope to send events and report metrics to HP Operations Manager (HPOM) and to Operations Management in BSM, and how to use SiteScope to send events and report metrics to NNMi.

Part IV Monitors

Describes how to work with SiteScope groups and monitors. It also describes how to monitor XML documents.

Part V Integration Monitors

Describes how to capture and forward data from third-party applications into BSM using SiteScope integration monitors. It also describes monitor field mapping and integration with Network Node Manager.

Part VI Remote Servers

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

Part VII Preferences

Describes how to configure the SiteScope's general and administrative functions, including infrastructure, integration, logs, settings for connecting to email, pager and SNMP systems, common event mappings, schedule profiles, user profiles, search and filter tags, and managing certificates and credentials. It also describes using SiteScope in an I18N environment and setting up the authentication strategy for logging into SiteScope.

Part VIII User-Defined Templates

Describes how to create and customize your own templates to efficiently deploy, maintain, and update monitoring solutions, including groups, monitors, remote servers, and alerts. It also describes automatically deploying a SiteScope template using an XML file.

Part IX Solution Templates

Describes how to deploy a predefined set of solution templates designed to monitor commonly used enterprise applications and network systems.

Part X SiteScope Dashboard

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

Part XI Alerts and Reports

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

Who Should Read This Guide

This guide is intended for the following users of SiteScope:

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

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

How Do I Find the Information That I Need?

This guide is part of the HP SiteScope Help. The SiteScope Help provides a single-point of access for all SiteScope documentation.

You can access the SiteScope Help by selecting **Help** > **SiteScope Help** on the SiteScope server.

Topic Types

Within this guide, each subject area is organized into topics. A topic contains a distinct module of information for a subject. The topics are generally classified according to the type of information they contain.

This structure is designed to create easier access to specific information by dividing the documentation into the different types of information you may need at different times.

Three main topic types are in use: **Concepts**, **Tasks**, and **Reference**. The topic types are differentiated visually using icons.

Topic Type	Description	Usage
Concepts 	Background, descriptive, or conceptual information.	Learn general information about what a feature does.
Tasks 	**Instructional Tasks.** Step-by-step guidance to help you work with the application and accomplish your goals. Some task steps include examples, using sample data. Task steps can be with or without numbering: ➤ **Numbered steps.** Tasks that are performed by following each step in consecutive order. ➤ **Non-numbered steps.** A list of self-contained operations that you can perform in any order.	➤ Learn about the overall workflow of a task. ➤ Follow the steps listed in a numbered task to complete a task. ➤ Perform independent operations by completing steps in a non-numbered task.
	Use-case Scenario Tasks. Examples of how to perform a task for a specific situation.	Learn how a task could be performed in a realistic scenario.

Topic Type	Description	Usage
Reference 	**General Reference**. Detailed lists and explanations of reference-oriented material.	Look up a specific piece of reference information relevant to a particular context.
	User Interface Reference. Specialized reference topics that describe a particular user interface in detail. Selecting **Help on this page** from the Help menu in the product generally opens the user interface topics.	Look up specific information about what to enter or how to use one or more specific user interface elements, such as a window, dialog box, or wizard.
Troubleshooting and Limitations 	**Troubleshooting and Limitations**. Specialized reference topics that describe commonly encountered problems and their solutions, and list limitations of a feature or product area.	Increase your awareness of important issues before working with a feature, or if you encounter usability problems in the software.

Additional Online Resources

Troubleshooting & Knowledge Base accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

HP Software Support accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

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 user ID, go to:

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

HP Software Web site accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

Documentation Updates

HP Software is continually updating its product documentation with new information.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

Part I

Introduction to SiteScope

1

Introducing SiteScope

This chapter includes:

Concepts

Concepts

SiteScope Overview

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

SiteScope monitors collect key performance measurements and report topology on a wide range of back-end infrastructure components. The monitors are individually configured to 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 can be configured to send alerts whenever it detects a problem in the IT infrastructure. In addition, SiteScope can create reports for monitors or monitor groups that display information about how the servers and applications you are monitoring have performed over time.

To help you deploy monitors with similar monitoring configuration criteria across the enterprise, you can define templates, or use preconfigured SiteScope solution templates. The use of templates enables you to develop and maintain a standardized set of monitor types and configurations in a single structure that can be repeatedly deployed and easily updated, without having to update to each object individually.

SiteScope also includes alert template types that you can use to communicate and record event information in a variety of media. You can customize alert templates to meet the needs of your organization.

Key Features of SiteScope

SiteScope has the following features:

- **Agentless monitoring.** SiteScope monitors without the deployment of agent software on the servers to be monitored. This function makes deployment and maintenance of SiteScope relatively simple compared to other performance monitoring solutions.
- **Simple installation and deployment.** SiteScope is installed on a single server running as a service or a process. This results in quick installation and easy monitoring configuration.
- **Intuitive administration.** SiteScope reduces the time spent managing a monitoring environment by providing a user friendly browser-based interface for viewing and administering of the monitoring platform. For details, see "Understanding the SiteScope User Interface" on page 64.
- **Enterprise-ready architecture.** SiteScope provides simultaneous monitoring of a large number of systems, support for secure connections, and failover capabilities. For details on SiteScope Failover Manager, see "Using SiteScope Failover Manager" on page 39.
- **Infrastructure performance and availability monitoring.** SiteScope has over 100 types of monitors. SiteScope can monitor utilization, response time, usage, and resource availability of a variety of host types and application platforms. For details on SiteScope monitors, see "SiteScope Monitors Overview" on page 392.
- **Standardized monitor deployments and updates using templates.** SiteScope supports the ability to create and publish reusable templates, enabling you to set up and deploy multiple IT elements with similar monitoring configuration criteria. Using the Publish Template Changes wizard, you can rapidly update your monitoring environment across the entire enterprise, without the need for extensive manual updates. For details on SiteScope templates, see "SiteScope Templates Overview" on page 944.
- **Automated deployment with XML.** SiteScope enables you to bypass the user interface and deploy templates using an XML file. This saves your IT organization time and money by enabling the introduction of a large number of monitors in a single operation. For details on auto template deployment, see "Auto Template Deployment Overview" on page 1054.

- **Baseline management.** SiteScope can be used to create baselines and schedule specific thresholds based on a time period or date. The baseline calculated for your configuration can be tested against actual performance conditions to view the errors and warnings that would have been reduced by the calculated baseline. Graphs can be used to compare your calculated baseline with current threshold settings to determine potential performance improvements. For details on using a baseline, see "Setting Status Thresholds Using a Baseline" on page 405.
- **Proactive alerting.** SiteScope can be configured to alert whenever it detects a problem in the IT infrastructure. There are several types of alert actions, such as sending email messages, paging, sending Simple Network Management Protocol (SNMP) traps, or executing a script. For details on SiteScope alerts, see "SiteScope Alerts Overview" on page 1417.
- **Server-based reporting.** SiteScope can collect multiple pre-selected metrics from a specific server and combine them into a single graph—giving you quick access to key performance monitoring data for any server in your environment. One of the key benefits of server-based reporting is the ability to drill down into reports to troubleshoot server related issues. For details on SiteScope reports, see "SiteScope Reports Overview" on page 1502.
- **Self-monitoring.** SiteScope monitors key aspects of its own operability and identifies monitor configuration problems and critical server load. It also monitors its own integration and data events when configured to report to Business Service Management. For details on monitoring SiteScope server health, see "SiteScope Health Overview" on page 1340.
- **Customization capabilities.** SiteScope permits the display of customizations of groups and monitors by using custom data fields and HTML-sensitive description tags. In addition, SiteScope permits the customization of alert text and report configurations by using templates and user-defined variables. For details, see "SiteScope Alert Template and Event Properties Directory" on page 1451.

- **Integrations.** SiteScope can be used to collect key performance metrics and to report topologies to BSM; send common events and metrics data to HP Operations Manager (HPOM) and to Operations Management in BSM using the HP Operations agent; send events and metrics data to Network Node Manager i (NNMi); and forward data to HP Diagnostics or to an application for which a direct integration does not exist. For details, see "SiteScope Integrations" on page 44.

SiteScope Monitoring Model

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

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

Part II

General and Administration

2

Setting Up and Administering SiteScope

This chapter includes:

Concepts

Tasks

Concepts

Getting Started Overview

This chapter provides an introduction for getting started with SiteScope, and a recommended flow for setting up and administering your monitoring solution.

For details on getting started, see "How to Get Started Using SiteScope" on page 48.

Using a Silent Login

Silent login is an automatic process that launches SiteScope without having to enter the user login name and password in the SiteScope login page. This enables you to skip the initial login page and instead go directly to a SiteScope client. In addition, you can use silent login in conjunction with a page option view that you saved in your browser's list of Favorites to open SiteScope directly to a particular group or view. For details on configuring a favorite page option view, see Page Options in "SiteScope Common Toolbar" on page 66.

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

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

For details on how to create a SiteScope silent login URL, see "How to Create a Silent Login URL" on page 51.

Using SiteScope Failover Manager

HP SiteScope Failover Manager is a special version of SiteScope that includes automated failover functionality. It automatically switches the functions of a primary system to a standby server if the primary system fails or is temporarily taken out of service.

Benefits of SiteScope Failover Manager include:

- SiteScope configuration sharing:
  - SiteScope is installed on a shared resource that is accessible to the failover machine.
  - When a primary SiteScope is down, the SiteScope Failover process activated by SiteScope Failover Manager continues monitoring from the exact point where the primary SiteScope left off.
  - No configuration copying (configuration changes between primary and failover servers are transparent), and configuration changes made on SiteScope Failover Manager are available on the primary SiteScope.
  - No data loss in reports.
- SiteScope Failover Manager installation:
  - Standalone management application with no user interface, that is responsible for managing primary and failover instances. It is installed on a local disk—not on the shared resource.
  - SiteScope Failover Manager can monitor multiple primaries simultaneously from a single Failover Manager machine, and provide automatic backup for a single SiteScope instance during failover.
  - The data storage requirements for SiteScope Failover are significantly less than for a primary SiteScope.
- SiteScope Failover Manager is freely included with your regular SiteScope installation.

For details on using SiteScope Failover Manager, see the *HP SiteScope Failover Manager Guide* PDF in <**SiteScope**>**\sisdocs\pdfs\SiteScopeFailover.pdf**.

Note: Since all primary SiteScopes must be installed on a shared resource, the installation paths referred to in this guide should be read as the SiteScope installation path on the shared resource.

Using the JMX Console

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

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

You can access the JConsole tool by running **<SiteScope root directory>\java\bin\jconsole.exe** on Windows platforms (and **<SiteScope root directory>/java/bin/jconsole** binary file on UNIX platforms). Depending on which SiteScope you want to monitor, select **Local**, or **Remote** with port **28006** (the default JMX port).

Tip:

- Since access to the JMX server is not password protected (JConsole password authentication is disabled by default in SiteScope), we recommend that you enable JMX password authentication to prevent unauthorized entry. For details, see "Enable JMX server password protection - optional" on page 58.
- We do not recommend changing any other JConsole settings.

Using the SiteScope Configuration API

SiteScope includes an extended SOAP-based API to help manage large and dynamic environments. This provides services for working with SiteScope templates, groups, monitors, alerts, remote servers, server health, search/filter tags, and configuration. Each API call can be run from the command line on a Windows or UNIX platform.

The following actions are supported using the SiteScope API:

SiteScope Object	Action
Templates	➤ Template management (create/delete template, create/delete template container, import template) ➤ Template deployment (monitor, group, alert, remote server creation) ➤ Update deployment (groups, monitors, alerts, remote server) using template update
Groups	Enable/disable groups, delete groups
Monitors	Enable/disable, delete monitors, run monitors
Alerts	Enable/disable alerts
Remote Servers	Delete remote server preferences
Status	Get SiteScope server status (active monitoring, booting) statistics
Tags	Create tags, add tag values, edit tag description, edit tag values (name, description), delete tags
Configuration	Get SiteScope configuration

SiteScope configuration API can be invoked by any known Web Services invocation framework such as Axis or WSIF, or by any client application. Using a SiteScope login name and password, you can call APIs and perform configuration changes and other actions.

The SiteScope API examples are available from the **<SiteScope installation directory>\examples\integrations\api** directory. See the **readme.txt** file in the **\api** directory for details on how to use the API.

For details of APIs included with SiteScope and sample Java code for utilizing the APIs, see the *HP SiteScope API Reference* located in **<SiteScope installation directory\examples\integrations\api\doc\javadoc.zip**.

Notes and Limitations

- The methods in this API require a SiteScope user and password as part of the method invocation. Before using these methods, edit the line of **<SiteScope installation>\groups\master.config** that defines access control to say "_accessControlled=true". The user and password can be in plain text or encrypted. To encrypt a string, use **<SiteScope installation>\tools\AutoDeployment\encrypt_password.bat**.
- All API methods that do not have a user name and password will be deprecated in future versions of SiteScope. All analogous API methods with user and password authentication have been renamed and now have an Ex suffix (for example, enableGroupEx) to avoid the same method names being used with different parameters.
- The access level of the SiteScope user affects the behavior of the methods. For example, when calling getConfigurationSnapshot and getFullConfigurationSnapshot, the returned maps contain only those entities that the user is privileged to access.
- To use applications created with previous versions of this API, set _accessControlled=false and use the deprecated APIs. These deprecated methods will not be supported in a future version and you will have to port your application to use the secure versions of the API methods.
- Attempting to use the deprecated forms of the methods when _accessControlled=true or to use the secure methods when _accessControlled=false results in an exception.

- The **.bat** files are examples only and not intended as production scripts. You can change the scripts to fit your requirements. Special characters are not supported in the parameter values.
- The disable alerts API is not supported when the **Disable alerts temporarily** permission is not selected in **Preferences** > **User Management Preferences** > **Permissions** > **Alerts**.
- Some API operations can be disabled on the server. This supports a read-only mode, such that the configuration cannot be changed remotely using the API.

SiteScope Integrations

SiteScope can be integrated with the following applications:

- **HP Business Service Management**. SiteScope can be used as a data collector for BSM. BSM receives data about end-users, business processes, and systems and uses the data in reports and analysis. You can configure SiteScope monitor data can be sent to BSM for all monitors, or for selected monitors only. For details, see "Working with Business Service Management (BSM)" on page 269.
- **HP Diagnostics.** Diagnostics monitors application servers using SiteScope. SiteScope forwards data about these application servers to Diagnostics providing an insight into the infrastructure components onto which the application servers are deployed. Diagnostics presents the data in its reports and graphs. For details, see "Diagnostics Integration Overview" on page 746.
- **HP Operations Manager.** SiteScope can work together with HP Operations Manager products to provide a combination of agentless, and agent-based infrastructure management. SiteScope uses the HP Operations agent:
  - To forward events data to HP Operations Manager (HPOM) or to Operations Management in BSM, enabling a more comprehensive and detailed overview of the health of your IT operation.
  - To act as data storage for metrics data collected by SiteScope, and make the data directly available to HPOM or Operations Management.

For details, see "Working with Operations Manager and BSM Using the HP Operations Agent" on page 307.

- **HP Network Node Manager** (NNMi). SiteScope can be used as a data collector for Network Node Manager i (NNMi), which is an event console used for network monitoring. SiteScope monitors the application side of the system that NNMi is monitoring, and uses SNMP Trap alerts to forward event data from any type of SiteScope monitor to NNMi. SiteScope can also report metrics data to NNMi. For details, see "Working with Network Node Manager i (NNMi)" on page 359.
- **Generic integrations.** SiteScope can be used to forward data to other applications that can receive the XML files that SiteScope forwards. These files contain information regarding the status of the SiteScope's groups, monitors, and measurements. For details on generic data integrations, see "Generic Data Integration Overview" on page 749. For a reference detailing the XML tags, elements, and attributes included in the integration file that SiteScope forwards to the receiving application, see "XML Tag Reference for Generic Data and Diagnostics Integrations" on page 753.

Tip: For best practices and troubleshooting for using and configuring the integration of SiteScope with BSM and HPOM products, see Best Practices for the SiteScope-BSM/OM Integration.

Using the SiteScope iPhone Application

The SiteScope iPhone application is a free download that enables you to keep track of your monitored IT infrastucture while away from your computer using iPhone, iPad, or iPod touch.

You can use the iPhone application to perform the following actions:

- Search SiteScopes to view monitor statistics, and perform actions on the search results to mitigate issues (view monitor details, enable/disable monitors, run monitors, set alert actions).
- Respond to email alerts when a problem is detected in the IT infrastructure (enable/disable alerts, enable/disable associated alerts, acknowledge alerts, view acknowledgement logs).
- Generate ad hoc reports for specific monitors, groups, or generated alerts, for a specific time period.
- Add selected monitors and groups to a favorites list.

The SiteScope iPhone application is available from the iPhone App Store (http://www.apple.com/iphone/apps-for-iphone/). For a movie demonstration of the SiteScope iPhone application, see http://www.youtube.com/watch?v=MuLAmO322nI.

For details on using SiteScope on an iPhone, refer to the help supplied with the SiteScope iPhone application.

For additional information on how to use the features that are available on the SiteScope iPhone application, see the relevant topic in the SiteScope Help.

This section also includes:

- "Configuration Requirements" on page 47
- "Notes and Limitations" on page 47

Configuration Requirements

- To configure alerts to be sent to an iPhone, use the **MobileAppMail** template in the <**SiteScope root**>\ **templates.mail** folder, as this template contains a link that can be used to open the application from your email.
- You need to include html content in mail templates sent to an iPhone. To enable this, set the value for the **_defaultMailAlertContentType** property to **=text/html** in the **master.config** file.
- To use SiteScope in secure mode on an iPhone, you must set the **_accessControlled** property to **=true** in the **master.config** file. Otherwise the SiteScope user name and password are ignored.
- Make sure the iPhone is set to the correct local time.

Notes and Limitations

- Monitors that are disabled for a temporary period of time (regardless of whether they were disabled in the SiteScope user interface or from an iPhone) are displayed in the monitor details summary according to server time.
- When deleting a SiteScope user account from your iPhone, any monitors or groups that are saved to favorites under that account will also be removed.
- When changing SiteScope user account settings (for example, changing a profile's protocol from http to https, or changing the SiteScope port), all monitors related to that profile disappear from the favorites list.
- If you encounter insufficient memory resource messages when generating a report, you should free up memory on the iPhone (for example, by closing running applications). You can increase or decrease the memory required by SiteScope reports by moving the **Minimum memory for reports (MB)** slider in iPhone Settings under HP SiteScope.
- If you are unable to connect the iPhone application to SiteScope using a 3G signal but you can connect using a wireless network (WiFi), try changing the SiteScope port to 80, as the service provider might be blocking some ports (such as the default SiteScope port, 8080).

Tasks

How to Get Started Using SiteScope

This task provides an overview of how to get started with SiteScope.

This task includes the following steps:

- "Install SiteScope" on page 48
- "Log on to SiteScope" on page 48
- "Manger SiteScope from the Configuration API - optional" on page 49
- "Set up and administer SiteScope" on page 49
- "Configure SiteScope to integrate with other applications - optional" on page 49
- "Configure SiteScope for monitoring" on page 49
- "Access SiteScope from an iPhone - optional" on page 49

1 Install SiteScope

You install SiteScope on a single server running as a service or a process with access to the applications and operating systems to be monitored. For details on installing SiteScope, see the HP SiteScope Deployment Guide PDF.

You can also install SiteScope Failover Manager for automated backup monitoring in case of a SiteScope failure. For details, see "Using SiteScope Failover Manager" on page 39.

2 Log on to SiteScope

To access SiteScope from a browser or from the Start menu, see "How to Access SiteScope" on page 50.

Alternatively, you can use silent login to skip the initial login page and go directly to a SiteScope client. For concept details, see "Using a Silent Login" on page 38. For task details, see "How to Create a Silent Login URL" on page 51.

3 Manger SiteScope from the Configuration API - optional

You can manage large and dynamic environments from the command line on a Windows or UNIX platform using the SiteScope Configuration API. For details, see "Using the SiteScope Configuration API" on page 42.

4 Set up and administer SiteScope

For a suggested working order for preparing to use SiteScope, see "How to Setup and Administer SiteScope" on page 55.

5 Configure SiteScope to integrate with other applications - optional

SiteScope can be used as a data collector for various other applications. For details, see "SiteScope Integrations" on page 44.

6 Configure SiteScope for monitoring

You can manually create a basic monitoring structure in SiteScope, or you can use SiteScope templates for mass deployments.

- To create a basic monitoring structure in SiteScope (by adding monitors individually into the groups you created), see "How to Configure SiteScope for Monitoring" on page 59.
- To use templates for standardizing the monitoring of different IT elements in your enterprise, see "How to Configure a SiteScope Monitoring Solution Using a Template – Flowchart" on page 62.

7 Access SiteScope from an iPhone - optional

To keep track of your monitored IT infrastructure and perform monitoring specific actions while away from your computer, you can use the SiteScope iPhone application. For details, see "Using the SiteScope iPhone Application" on page 46.

How to Access SiteScope

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

This task includes the following steps:

Access SiteScope from a browser - optional

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

Access SiteScope from the Start menu - optional

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

Access SiteScope using remote login - optional

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

For concept details, see "Using a Silent Login" on page 38.

For task details, see "How to Create a Silent Login URL" on page 51.

Results

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

Note: To restrict access to this account and its privileges, you need to edit the Administrator account profile to include a user login name and login password. SiteScope then displays a login dialogue before SiteScope can be accessed. If no user name and password are defined for the Administrator user, SiteScope skips the login page and automatically logs in. For details on editing the Administrator account profile, see "User Management Preferences Overview" on page 846.

How to Create a Silent Login URL

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

This task includes the following steps:

1 Create a user profile

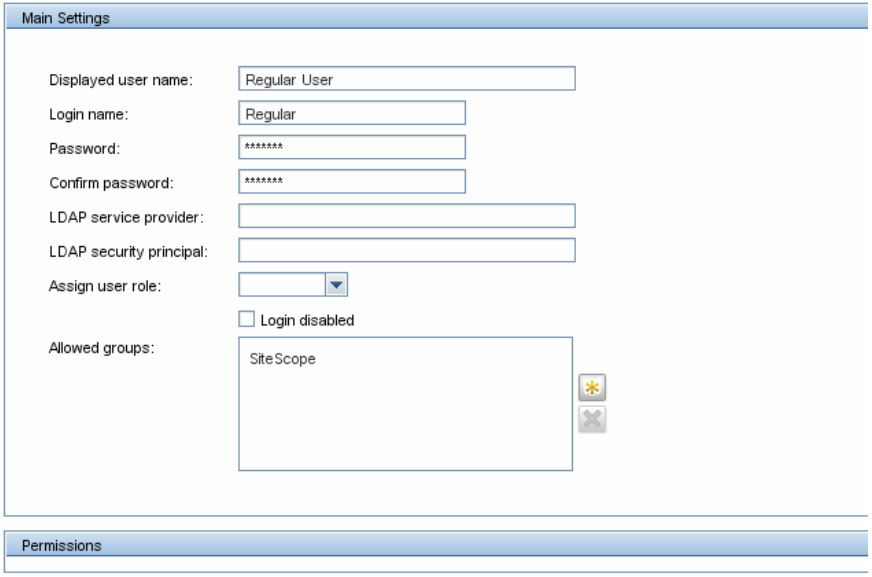
In the **Preferences** context, click the **User Management Preferences** menu and create a user account.

For user interface details, see "User Management Preferences Page" on page 864.

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

Example:

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



2 Configure user permissions - optional

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

For user interface details, see "New/Edit User Profile Dialog Box" on page 870.

3 Encrypt the user profile

Encrypt the user login name and password.

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

For example:
C:\SiteScope\tools\AutoDeployment\encrypt_password.bat Regular

The encrypted value for Regular is (sisp)uq1zrGl1lms=.

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

In this example, = is a reserved character, and should be replaced by %3D. Thus, the encoded value for Regular is (sisp)uq1zrGl1lms%3D.

c Save the encrypted value so that you can add it to the silent login URL.

d Repeat the encryption process for the login password (if different from the login name).

4 Create a SiteScope silent login URL for the user profile

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

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

where <encrypted_login_name> and <encrypted_password> are replaced by the encrypted login name and password.

5 Results

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

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

How to Setup and Administer SiteScope

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

Note for users working with SiteScope Failover Manager: If you are using SiteScope Failover Manager to provide backup infrastructure monitoring availability, see the *HP SiteScope Failover Manager Guide* PDF located in **<SiteScope root directory>\sisdocs\pdfs\SiteScopeFailover.pdf** for a suggested working order.

This task includes the following steps:

1 Log on to SiteScope

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

2 Enter your SiteScope license

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

For user interface details, see "License file" on page 698.

3 Configure SiteScope preferences

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

a **Create a SiteScope user account.** The Administrator account is the default account that is active when the product is installed. It has full privileges to manage SiteScope and is the account that all users who access the product use unless you restrict the account. Create and configure other user accounts based on the requirements of the organization. For task details, see "How to Create a SiteScope User Profile" on page 853.

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

---

b **Configure the SiteScope Email Preferences server.** Configure an administrators email address and specify a mail server that SiteScope can use to forward email messages and alerts to users. For user interface details, see "Email Preferences Page" on page 793.

c **Adjust Log Preferences.** Set the number of days of monitor data that are retained on the SiteScope server. By default, SiteScope deletes logs older than 40 days. If you plan to have monitor data exported to an external database, prepare the database, the necessary drivers, and configure the Log Preferences as applicable. For user interface details, see "Log Preferences Page" on page 786.

d **Configure credentials for SiteScope objects.** Use Credential Preferences to store and mange credentials for SiteScope objects that require user authentication. For task details, see "How to Configure Credential Preferences" on page 895.

e **Configure SiteScope integrations** (as required).

- Configure SiteScope to report to BSM. This enables logging of SiteScope monitor data and topology reporting to BSM. For task details, see "How to Configure the Integration Between SiteScope and BSM" on page 288.

- Configure the HP Operations Manager (HPOM) integration. This enables sending SiteScope events and reporting metrics data to HPOM and BSM products. For task details on sending events to HPOM and BSM, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326. For task details on reporting metrics to HPOM and BSM, see "How to Enable SiteScope to Report Metrics to the HP Operations Agent" on page 349.

- Configure the HP Diagnostics integration. This enables you to see a more complete view of the application servers that are monitored by Diagnostics. For user interface details, see "Diagnostics Integration Preferences Dialog Box" on page 771.

- Configure the generic data integration. This enables you to forward SiteScope data to an application for which a direct integration does not exist. For user interface details, see "Data Integration Preferences Dialog Box" on page 766.

- Configure the Network Node Manager i (NNMi) integration. This enables sending SiteScope events and reporting metrics data to NNMi. For task details on sending events to NNMi, see "How to Configure SiteScope to Send Event Data to NNMi" on page 364. For task details on reporting metrics to NNMi, see "How to Configure SiteScope to Report Metrics Data to NNMi" on page 367.

f In addition, you can configure any of the other SiteScope preferences as required. For details, see "Preferences Menu" on page 104.

4 Configure connection profiles for remote servers

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

For details on enabling SiteScope to monitor data on remote Windows servers, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.

For details on enabling SiteScope to monitor data on remote UNIX servers, see "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

5 Install middleware drivers (if required)

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

For details, see the help for the specific monitor.

6 Enable JMX server password protection - optional

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

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

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

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

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

For details on configuring the JVM, see the Java Oracle documentation, http://download.oracle.com/javase/1.5.0/docs/guide/management/agent.html.

For details on the JMX Console, see "Using the JMX Console" on page 40.

7 Results

You are now ready to use SiteScope.

➤ For details on creating a basic monitoring structure in SiteScope, see "How to Configure SiteScope for Monitoring" on page 59.

➤ For details on how to create and develop templates to help speed the deployment of monitoring using standardized group structure, naming conventions, and configuration settings, see "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964.

How to Configure SiteScope for Monitoring

This task describes the working order for creating a basic monitoring structure in SiteScope by adding monitors individually into the groups you created.

Tip: Alternatively, you can use SiteScope templates, solution templates, the Publish Template Changes wizard, or automatic template deployment for standardizing the monitoring of the different IT elements in your enterprise. These methods are more efficient than the basic monitoring method for mass deployments. For a flowchart that shows the steps involved in configuring a monitoring solution using a template, see "How to Configure a SiteScope Monitoring Solution Using a Template – Flowchart" on page 62.

For details on the template workflow, see "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964.

This task includes the following steps:

1 Prerequisites

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

For task details, see "How to Setup and Administer SiteScope" on page 55.

2 Create groups and subgroups

Create groups according to the monitor hierarchy which you want to implement. This enables you to make deployment of monitors and associated alerts manageable and effective for your environment and organization. For example, you can create groups of locations, server types, network resources, and so forth.

For task details, see "How to Manage a Group" on page 383.

3 Create monitor instances

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

For task details, see "How to Deploy a Monitor" on page 414.

4 Set monitor dependencies - optional

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

For concept details, see "Monitoring Group Dependencies" on page 397.

5 Set monitor thresholds - optional

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

➤ For task details on how to set monitor thresholds using a baseline, see "How to Set Monitor Thresholds Using a Baseline" on page 418.

➤ For user interface details for setting monitor thresholds manually, see "Threshold Settings" on page 457.

6 Set up monitor and group alerts - optional

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

For task details, see "How to Configure an Alert" on page 1443.

7 Set up monitor and group reports - optional

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

For task details, see "How to Create a Report" on page 1508.

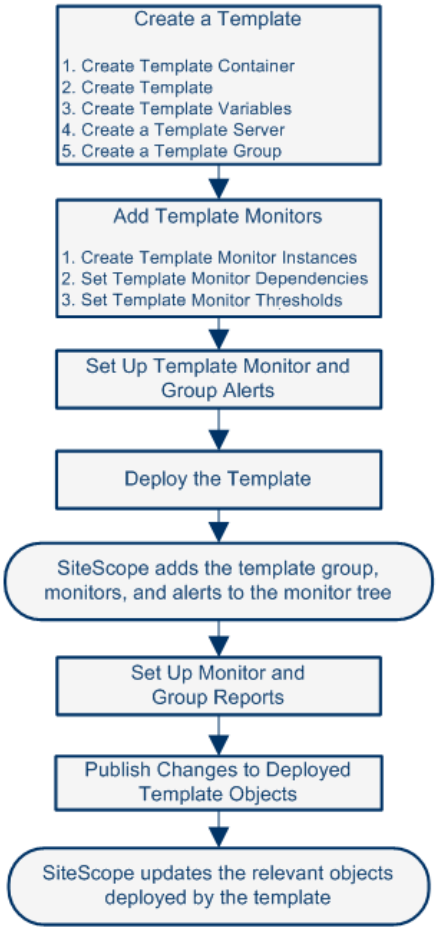
8 Results

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

How to Configure a SiteScope Monitoring Solution Using a Template – Flowchart

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

For details on the workflow, see "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964.



3

Navigating the SiteScope User Interface

This chapter includes:

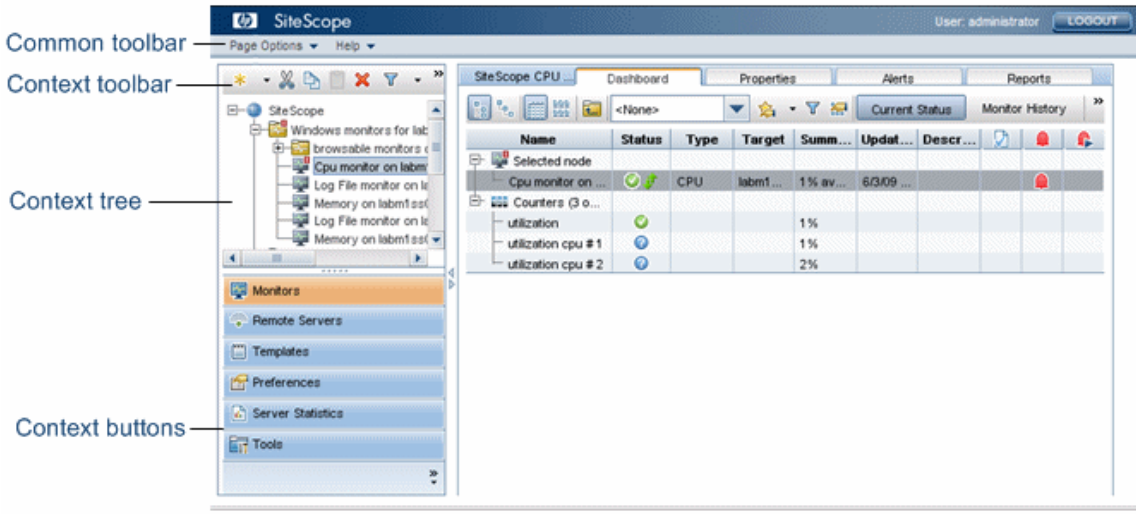
Concepts

Reference

Concepts

Understanding the SiteScope User Interface

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



The SiteScope window contains the following key elements:

- **SiteScope common toolbar.** Provides access to page options, documentation, and additional resources. This toolbar is located on the upper part of the window. For more details, see "SiteScope Common Toolbar" on page 66.
- **SiteScope context toolbars.** Contains buttons for frequently-used commands in the selected SiteScope context. For more details, see "Tree Toolbar Buttons" on page 74.
- **SiteScope context tree.** Enables you to create and manage SiteScope objects in a tree structure. For details, see "Monitor Tree" on page 81, "Remote Server Tree" on page 93, and "Template Tree" on page 95.

➤ **SiteScope context buttons.** Provide access to the SiteScope Monitors, Remote Servers, Templates, Preferences, Server Statistics, and Diagnostic Tools. For more details, see "SiteScope Context Buttons" on page 67.

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

This section also includes:

SiteScope Common Toolbar

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

UI Element	Description
Page Options	Enables you to select the following page options: ➤ **Add to Favorites.** Enables you to add the current SiteScope view to your list of Favorites in your browser. ➤ **Save Layout to User Preferences.** Enables you to save the current view as the default layout for the specific SiteScope user.
Help	Enables you to access SiteScope Help, context-sensitive help for specific windows, release notes, and other additional online resources. You can also see descriptions of user interface elements in most pages or dialog boxes. To enable this feature, click the **Quick Help** button in the specific page or dialog box, and rest the mouse pointer on the element box to display a ToolTip description. Click the **Quick Help** button again to make this feature unavailable.
LOGOUT	Logs you out of your SiteScope session.

You can customize your view of the monitor tree to list only those SiteScope elements with which you are working. You can also assign search/filter tags to your groups, monitors, reports, and alerts to further refine your selection. For details on this topic, see "Searching and Filtering SiteScope Objects Overview" on page 116.

SiteScope enables you to change monitor configurations across multiple monitors, groups, or multiple SiteScopes using Global Replace. For details on the Global Replace user interface, see "Global Search and Replace Wizard" on page 142.

SiteScope Context Buttons

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

UI Element	Description
	Enables you to create and manage SiteScope groups and monitors in a hierarchy represented by a monitor tree. For user interface details, see "Monitor Tree" on page 81.
	Enables you to set up the connection properties so that SiteScope can monitor systems and services running in remote Windows and UNIX environments. For user interface details, see "Remote Server Tree" on page 93.
	Enables you to use templates to deploy a standardized pattern of monitoring to multiple elements in your infrastructure. You can use preconfigured SiteScope solution template or create and manage your own templates. For user interface details, see "Template Tree" on page 95.
	Enables you to configure specific properties and settings related to most of the administrative tasks within SiteScope. For user interface details, see "Preferences Menu" on page 104.
	Enables you to view key SiteScope server performance metrics. For user interface details, see "Server Statistics Menu" on page 106.
	Displays diagnostic tools that can help you troubleshoot problems in SiteScope and facilitate monitor configuration. For details on the available tools, see "SiteScope Tools Overview" on page 160.

Navigating and Performing Actions in the Context Tree

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

You can perform actions using the context toolbar, or you can select any object within the context tree itself, and right-click the object to access a menu of options for that object. For example, if you right-click the SiteScope node in the monitor tree, you select from a menu listing only those actions that can performed on the SiteScope node. You can also perform actions on multiple groups and monitors. For details, see "Performing Actions on Multiple Groups and Monitors" on page 68.

For details of the context tree objects and context menu options available for each object in the tree, see "Monitor Tree" on page 81, "Remote Server Tree" on page 93, "Template Tree" on page 95, "Preferences Menu" on page 104, "Server Statistics Menu" on page 106, and "Tools Menu" on page 108.

Performing Actions on Multiple Groups and Monitors

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

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

For user interface details, see "Manage Monitors and Groups Dialog Box" on page 77.

Copying and Moving SiteScope Objects

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

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

You can copy or move the following SiteScope objects:

SiteScope Object	Action and Description
Group	**Copy/Paste.** Copy a monitor group, including its subgroups, monitors, alerts, and reports, to the same or a different monitor group. **Cut/Paste.** Move a monitor group, including its subgroups, monitors, alerts, and reports, to a different monitor group. **Copy to Template.** Copy a monitor group, including its monitors, alerts, and reports, to a template. **Note:** ➤ You cannot move or copy a monitor group to its subgroup. ➤ If you move a group that is targeted by an alert or report without also moving the alert or report, the group is removed from the alert or report target. ➤ Baseline thresholds are not copied or moved with a monitor whose thresholds were set using the baseline.

SiteScope Object	Action and Description
Monitor	**Copy/Paste.** Copy a monitor, including its alerts and reports, to the same or a different monitor group. **Cut/Paste.** Move a monitor, including its alerts and reports, to a different monitor group. **Copy to Template.** Copy a monitor, including its alerts and reports, to a template. **Note:** ➤ If you move a monitor that is targeted by an alert or report without also moving the alert or report, the monitor is removed from the alert or report target. ➤ After copying a monitor, you normally need to change the system or application that the monitor is targeting, otherwise the copied monitor duplicates the monitoring actions of the original monitor instance. ➤ Baseline thresholds are not copied or moved with a monitor whose thresholds were set using the baseline.
Remote Server	**Copy to Template.** Copy a remote server profile to a template.
Template Container	**Paste/Paste.** Copy a template container and paste it to another template container or to the SiteScope root.
Template	**Copy/Paste.** Copy a template including its groups, monitors, alerts, and report, to a template container.
Template Group	**Copy/Paste.** Copy a template group including its subgroups, monitors, alerts, and reports to a template (provided the template does not already contain a template group) or to a template group.
Template Monitor	**Copy/Paste.** Copy a template monitor including its alerts and reports to a template group.
Alert	**Copy/Paste.** Copy an alert definition (from the Alerts tab) to the same or a different location (group or monitor) in the monitor tree or template tree.
Report	**Copy/Paste.** Copy a report definition (from the Reports tab) to the same or a different location (group or monitor) in the monitor tree or template tree.

Note: You can also move or copy multiple monitors and groups to a target group by clicking the **Manage Monitors and Groups** button in the monitor tree toolbar. For user interface details, see "Manage Monitors and Groups Dialog Box" on page 77.

For details on copying or moving SiteScope objects, expand the context menu option for the relevant SiteScope view in "Navigating SiteScope User Interface" on page 73.

Reference

SiteScope Keyboard Shortcuts

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

UI Element	Description
CTRL+A	Opens the New Alert dialog box, enabling you to create a new alert. For user interface details, see "New/Edit Alert Dialog Box" on page 1463.
CTRL+C	Copies the selected item and puts it on the Clipboard.
CTRL+D	Deletes the selected item.
CTRL+F	Opens the New Filter dialog box, enabling you to create a new filter. For user interface details, see "New/Edit Filter Dialog Box" on page 123.
CTRL+G	Opens the New Group dialog box, enabling you to create a new group. For user interface details, see "New SiteScope Group Dialog Box" on page 387.
CTRL+J	Opens the Select Template/Group dialog box, enabling you to select the template that you want to deploy or the group to which you want to deploy a template. For details on the Select Template user interface, see "Select Template Dialog Box" on page 488. For details on the Select Group user interface, see "Select Group Dialog Box" on page 1022.
CTRL+M	Opens the New Monitor dialog box, enabling you to add a new monitor. For user interface details, see "New Monitor Dialog Box" on page 444.
CTRL+R	Clears the filter configured in the Filter dialog box. For user interface details, see "New/Edit Filter Dialog Box" on page 123.

UI Element	Description
CTRL+V	Pastes the contents of the Clipboard to the selected location.
CTRL+X	Cuts the selected item and puts it on the Clipboard.
DELETE	Deletes the selection.
F5	Refreshes the tree.

Navigating SiteScope User Interface

This section includes:

Tree Toolbar Buttons

The tree toolbars enable you to perform common functions in the different SiteScope views.

To access	Select the **Monitors/Remote Servers/Templates** context. The tree toolbar is displayed above the upper left pane.
Important information	Some toolbar buttons are not available in all SiteScope views
See also	➤ "Monitor Tree" on page 81 ➤ "Remote Server Tree" on page 93 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
	**New.** Adds SiteScope objects (groups, monitor, alerts, remote servers, and templates) to the relevant tree. The objects that you can add depend on the context.
	**Test.** Tests the connection to the server. **Note:** Available in the remote server tree toolbar only.
	**Detailed Test.** Runs a test that displays the result of running commands on the remote server. This enables checking the permissions for the defined user. **Note:** Available in the remote server tree toolbar for UNIX servers only.
	**Cut.** Moves the selected object to another location in the tree.
	**Copy.** Makes a copy of the selected object.
	**Paste**. Copies or moves an object to the selected location in the tree.
	**Delete.** Deletes the selected object from the tree.

UI Element	Description
	**Filter.** Filters the monitor tree to display only those SiteScope objects that meet the criteria that you define. Select a filter option: ➤ **New Filter.** Opens the New Filter dialog box which enables you to create a filter. For user interface details, see "New/Edit Filter Dialog Box" on page 123. ➤ **Clear Filter.** Clears the filter settings. ➤ **<List of existing filters>.** Displays a list of existing filters. The following options are available: ➤ **Apply.** Applies the filter to the left tree pane. ➤ **Edit.** Opens the Edit Filter dialog box which enables you to edit the filter. For user interface details, see "New/Edit Filter Dialog Box" on page 123. ➤ **Delete.** Deletes the filter from the filter list. **Note:** Available in the monitor tree toolbar only.
	**Manage Monitors and Groups.** Enables you to perform an action (copy, move, delete, run monitors, enable/disable monitors, enable/disable associated alerts) on multiple groups and monitors in the monitor tree. You can also filter the list of objects in the monitor tree. For details on the Manage Monitors and Groups dialog box, see "Manage Monitors and Groups Dialog Box" on page 77. **Note:** Available in the monitor tree toolbar only.
	**Refresh.** Refreshes the data in the tree.
	**Collapse All.** Collapses all branches in the tree. **Note:** Available in the monitor and template tree toolbar only.
	**Expand All.** Expands all branches in the tree. **Note:** Available in the monitor and template tree toolbar only.

UI Element	Description
	**Show/Hide Pane.** Shows or hides the tree, and expand or contract the right pane.
	Click to configure the context button display. The following options are available: ➤ **Show More Buttons.** Click to show the next highest ranking SiteScope context button in the left pane. This button is available only if not all the context buttons are displayed. ➤ **Show Fewer Buttons.** Click to hide the lowest ranking SiteScope context button from the left pane. This button is available only if at least one context buttons is displayed. ➤ **Option.** Choose the order in which the SiteScope context buttons are displayed. Use the **Move Up** and **Move Down** buttons to rearrange the order. To hide a button from the left pane, clear the check box for the context. By default, all the context buttons are selected (displayed in the left pane). ➤ **Add or Remove Buttons.** Shows the show/hide status of the context buttons. By default, all the context buttons are selected (displayed in the left pane). To hide a button, clear the check mark for the context.

Manage Monitors and Groups Dialog Box

This dialog box enables you to select one or more groups, monitors, or both, and perform an action on the selected objects (copy, move, delete, run monitors, enable/disable monitors, enable/disable associated alerts). You can also use the filter options to create a filtered list of groups and monitors based on a filter criteria, or select an existing filter previously defined in the monitor tree filter.

To access	Select the **Monitors** context. In the monitor tree toolbar, click the **Manage Monitors and Groups** button.
Important information	➤ The toolbar actions are available according to the user permissions and the objects selected. ➤ The Health container cannot be deleted.
Relevant tasks	➤ "How to Manage a Group" on page 383 ➤ "How to Deploy a Monitor" on page 414 ➤ "How to Create and Define a New Search/Filter Tag" on page 119
See also	"Performing Actions on Multiple Groups and Monitors" on page 68

User interface elements are described below:

UI Element	Description
	**Filter.** Enables you to filter the monitor tree to display only those SiteScope objects that meet the criteria that you define. After applying a filter, the name of the filter is displayed in the button (**custom**, if the filter was created in the Manage Monitors and Groups dialog box; otherwise the name of the filter defined in the monitor tree filter). Click the **Filter** button arrow and select a filter option: ➤ **New Filter.** Opens the New Filter dialog box which enables you to create a filter. For user interface details, see "New/Edit Filter Dialog Box" on page 123. ➤ **Clear Filter.** Clears the filter settings. ➤ **<List of existing filters>.** Displays a list of existing filters previously defined in the monitor tree filter.
	**Select All.** Selects all listed SiteScope objects.
	**Clear Selection.** Clears the selection.
	**Cut.** Moves the selected objects to the destination group. **Note:** ➤ Any alerts defined for a specific monitor are transferred with the monitor. ➤ Moving a monitor restarts its history and any reports generated for the monitor are started from the time that the monitor was moved. The history data is still in the log files, but it is inaccessible from the reports for the monitor after it has been moved. Moving groups has no effect on history. ➤ Moving a monitor may break group-to-monitor dependencies. If you have one or more groups dependent on the status of the monitor you are moving, you should update that dependency after moving the monitor.

UI Element	Description
	**Copy.** Makes a copy of the selected objects for pasting to the destination group.
	**Paste.** Pastes the selected objects to the destination group. If you make a copy of a SiteScope object and it has the same name as an existing object in the container, SiteScope automatically adds a suffix (number) to the end of the object's name. **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).
	**Delete.** Deletes the selected objects from the monitor tree.
	**Run Monitors.** Runs the monitor or any monitors configured in the group. This opens an information window with the results.
	**Enable/Disable Monitor.** Opens the Enable/Disable Monitor dialog box which enables you to enable or disable the monitor or all the monitors in the group, regardless of the setting in the monitor properties. If you select **Disable**, the monitors are disabled until you return to this dialog box and select **Enable**. For user interface details, see "Enable/Disable Monitors in Group Dialog Box" on page 1321.

UI Element	Description
	**Enable/Disable Associated Alerts.** Open the Enable/Disable Associated Alerts dialog box which enables you to enable or disable all alerts associated with the monitor or all monitors in the group. For more details, see "Enable/Disable Associated Alerts" on page 482.
<SiteScope objects>	Actions are applied to all monitors and groups that are selected using the check box selections in the tree. The display of the tree is saved across visits to the dialog box and the actions associated with it. ➤ To select an object, select the check box to the left of the object name. Any combination of groups or monitors can be selected. A ▣ icon displayed to the left of a group indicates that not all monitors and subgroups contained within that group have been selected. ➤ To select a destination for copying or moving an object, click the object name (not the check box). **Default value:** The top level groups are shown, but no objects are selected.

Monitor Tree

The monitor tree represents the organization of systems and services in your network environment. The tree includes containers and objects within your infrastructure. The shortcut menu options include descriptions of the context menu options available for each object in the monitor tree.

To access	Select the **Monitors** context. The monitor tree is displayed in the left pane.
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. ➤ You can search for objects in the monitor tree by selecting a node and typing the characters you want to search in the popup search box. Click the ESC key to close the search box.
See also	"Working with SiteScope Monitors" on page 391

Monitor Tree Objects

User interface elements are described below:

UI 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 SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors). If an alert has been set up for the monitor group or subgroup, the alert symbol is displayed next to the group icon. If a Management report has been set up for the monitor group or subgroup, the report symbol is displayed next to the group icon. **Parent:** SiteScope or SiteScope group. **Add to tree by:** Creating, or importing with a SiteScope that has groups defined.

UI Element	Description
	Represents a SiteScope monitor (enabled/disabled). If an alert has been set up for the monitor, the alert symbol is displayed next to the monitor icon. If a Management report has been set up for the monitor, the report symbol is displayed next to the monitor icon. **Parent:** SiteScope group or subgroup, template, or solution template. **Add to tree by:** Creating, or importing with a SiteScope that has monitors configured.
	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.

SiteScope Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Baselining	Enables you to create a baseline for monitoring variations in response times and performance in the infrastructure for all monitors under SiteScope. ➤ **Calculate.** Enables you to select monitors and specify the relevant time and schedule to be used for calculating the baseline. It also enables you to select and fine-tune the baseline adherence level and define boundaries. ➤ **Review & Activate.** Displays a summary of calculated monitors and baseline data. It also enables you to save the current monitor configuration, view and retry failed operations, view baseline measurement graphs, and apply the baseline configuration. ➤ **Remove.** Enables you to remove the baseline threshold or recalculate the baseline after a baseline has been calculated. ➤ **Status Report.** Displays information about the baseline status for all monitors under SiteScope. For details on this topic, see "Setting Status Thresholds Using a Baseline" on page 405.
Deploy Template	Opens the Select Template dialog box that enables you to select a template to deploy to the group. For user interface details, see "Select Template Dialog Box" on page 488.
Deploy Template Using CSV	Opens the Select Template dialog box which enables you to select a template to deploy to the group using a CSV file. For user interface details, see "Select Template Dialog Box" on page 488.
Expand All	Opens all the subtrees under SiteScope.

Menu Item (A-Z)	Description
Global Search and Replace	Opens the Global Search and Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details on this topic, see "Global Search and Replace Wizard" on page 142.
Monitor Deployment Wizard	This menu item is available only to those users accessing SiteScope from System Availability Management Administration (SAM Admin) in BSM. Opens the Monitor Deployment Wizard. For details on this topic, see "Monitor Deployment Wizard" in *Using System Availability Management* in the HP Business Service Management Documentation Library.
New > Alert	Opens the New Alert window which enables you to define a new alert for SiteScope. For details on this topic, see "SiteScope Alerts" on page 1415.
New > Group	Opens the New Group window which enables you to define a new SiteScope group. For user interface details, see "New SiteScope Group Dialog Box" on page 387.
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 SAM Admin when there is more than one SiteScope connected to BSM. Pastes the selected SiteScope object (that was previously copied or cut) from another SiteScope to the SiteScope node.
Reports > Management/Quick/ Monitor/Alert	Enables you to select the type of SiteScope report you want to define. For details on these reports, see "SiteScope Reports" on page 1501.

Menu Item (A-Z)	Description
Reports > **BSM Configuration Changes**	This menu item is available only through SAM Admin when the SiteScope is connected to BSM. Displays a log of configuration changes made to BSM. For details, see "SiteScope Report Types" on page 1504.
Tools	Available when configuring or editing specific monitors (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). If a tool is available, click to open and run the tool with the monitor's existing data as its input. The test results are displayed in the **Results** pane. For details on the available tools, see "SiteScope Tools Overview" on page 160.

Group Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Baselining	Enables you to create a baseline for monitoring variations in response times and performance in the infrastructure for all monitors in the group. ➤ **Calculate.** Enables you to select monitors from the group and specify the relevant time and schedule to be used for calculating the baseline. It also enables you to select and fine-tune the baseline adherence level and define boundaries. ➤ **Review & Activate.** Displays a summary of calculated monitors and baseline data for the group. It also enables you to save the current monitor configuration, view and retry failed operations, view baseline measurement graphs, and apply the baseline configuration. ➤ **Remove.** Enables you to remove the baseline threshold or recalculate the baseline after a baseline has been calculated. ➤ **Status Report.** Displays information about the baseline status for all monitors in the group. For details on this topic, see "Setting Status Thresholds Using a Baseline" on page 405.
Copy	Copies the group and its contents (monitors, alerts, and reports) to a monitor group or template. **Note:** When copying a group that contains monitors with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitors are no longer in baseline mode.
Copy to other SiteScope	This menu item is available only through SAM Admin when there is more than one SiteScope connected to BSM. Copies the group and its contents (monitors, alerts, and reports) from another SiteScope to a monitor group or template in the SiteScope node.

Menu Item (A-Z)	Description
Copy to Template	Copies the group and its contents (monitors, alerts, and reports) to a template group. For details on this topic, see "How to Create a Template by Copying Existing Configurations" on page 973.
Cut	Moves the group and its contents (monitors, alerts, and reports) or a monitor and its contents (alerts and reports) to a monitor group. **Note:** When moving a group that contains monitors with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitors are no longer in baseline mode.
Delete	Deletes the group. **Note:** You cannot delete a group if it has dependent alerts or reports at the container level. To delete a group with dependencies, you must remove the group from **Alert Targets** and **Report Targets** for each dependency, and then delete the group. You can delete groups that have dependencies at the child level.
Deploy Template	Opens the Select Template dialog box that enables you to select a template to deploy to the group. For user interface details, see "Select Template Dialog Box" on page 488.
Deploy Template Using CSV	Opens the Select Template dialog box which enables you to select a template to deploy to the group using a CSV file. For user interface details, see "Select Template Dialog Box" on page 488.
Enable/Disable Monitor	Opens the Enable/Disable Monitors in Group dialog box which enables you to enable or disable monitors in the group, regardless of the setting in the monitor properties. If you select **Disable**, the monitors are disabled until you return to this dialog box and select **Enable**. For details on the Enable/Disable Monitor user interface, see "Enable/Disable Monitors in Group Dialog Box" on page 1321.

Menu Item (A-Z)	Description
Expand All	Opens all the subtrees under the group.
Global Search and Replace	Opens the Global Search and Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details on this topic, see "Global Search and Replace Wizard" on page 142.
Monitor Deployment Wizard	This menu item is available only to those users accessing SiteScope from SAM Admin in BSM. Opens the Monitor Deployment Wizard. For details on this topic, see "Monitor Deployment Wizard" in *Using System Availability Management* in the HP Business Service Management Documentation Library.
New > Alert	Opens the New Alert window which enables you to define a new alert for the group. For details on this topic, see "SiteScope Alerts" on page 1415.
New > Group	Opens the New Group window which enables you to define a new SiteScope group. For user interface details, see "New SiteScope Group Dialog Box" on page 387.
New > Monitor	Opens the New Monitor window which enables you to define a new SiteScope monitor. For user interface details, see "New Monitor Dialog Box" on page 444.
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 SAM Admin when there is more than one SiteScope connected to BSM. 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.

Menu Item (A-Z)	Description
Reports	Enables you to select the type of SiteScope report you want to define. For details on this topic, see "SiteScope Reports" on page 1501.
Run Monitors	Runs any monitors configured in the group, and opens an information window with the results.

Monitor Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Baselining	Enables you to create a baseline for monitoring variations in response times and performance in the infrastructure for the specific monitor. ➤ **Calculate.** Enables you to select the monitor and specify the relevant time and schedule to be used for calculating the baseline. It also enables you to select and fine-tune the baseline adherence level and define boundaries. ➤ **Review & Activate.** Displays a summary of the calculated monitor's baseline data. It also enables you to save the current monitor configuration, view and retry failed operations, view baseline measurement graphs, and apply the baseline configuration. ➤ **Remove.** Enables you to remove the baseline threshold or recalculate the baseline after a baseline has been calculated. ➤ **Status Report.** Displays information about the monitor's baseline status. For details on this topic, see "Setting Status Thresholds Using a Baseline" on page 405.

Menu Item (A-Z)	Description
Copy	Copies the monitor and its contents (alerts and reports) to a monitor group or template. **Note:** When copying a monitor with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitor is no longer in baseline mode.
Copy to other SiteScope	This menu item is available only through SAM Admin when there is more than one SiteScope connected to BSM. Copies the monitor and its contents (alerts and reports) from another SiteScope to a monitor group or template.
Copy to Template	Copies the monitor and its contents (alerts and reports) to a template group. For details on this topic, see "How to Create a Template by Copying Existing Configurations" on page 973.
Cut	Moves the monitor and its contents (alerts and reports) to a monitor group. **Note:** When moving a monitor with baseline thresholds, the baseline thresholds are replaced with static thresholds (which are the current percentile values), and the monitor is no longer in baseline mode.
Delete	Deletes the monitor. **Note:** You cannot delete a monitor if it has dependent alerts or reports at the container level. To delete a monitor with dependencies, you must remove the monitor from **Alert Targets** and **Report Targets** for each dependency, and then delete the monitor. You can delete monitors that have dependencies at the child level.
Enable/Disable Monitor	Opens the Enable/Disable Monitors in Group dialog box which enables you to enable or disable the monitor, regardless of the setting in the monitor properties. If you select **Disable**, the monitor is disabled until you return to this dialog box and select **Enable**. For details on the Enable/Disable Monitor user interface, see "Enable/Disable Monitors in Group Dialog Box" on page 1321.

Menu Item (A-Z)	Description
Global Search and Replace	Opens the Global Search and Replace Wizard, which enables you to run a global search and replace for monitor, alert, group, preferences, alert action, and report properties. For details on this topic, see "Global Search and Replace Wizard" on page 142.
New > Alert	Opens the New Alert window which enables you to define a new alert for the monitor. For details on this topic, see "SiteScope Alerts" on page 1415.
Paste	Pastes the selected monitor context object to the specified monitor.
Paste from other SiteScope	This menu item is available only through SAM Admin when there is more than one SiteScope connected to BSM. Pastes the selected monitor context object from another SiteScope to the specified monitor.
Reports	Enables you to select the type of SiteScope report you want to define. For details on this topic, see "SiteScope Reports" on page 1501.
Run Monitor	Runs the monitor and opens an information window with the results.

SiteScope Health Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Disable Logging	Disables logging on SiteScope Health. For details, see "SiteScope Server Health" on page 1339.
Enable Logging	Enables logging on SiteScope Health. For details, see "SiteScope Server Health" on page 1339.
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. For details on this topic, see "SiteScope Alerts" on page 1415.

Menu Item (A-Z)	Description
New > Group	Opens the New Group window which enables you to define a new SiteScope group. For user interface details, see "New SiteScope Group Dialog Box" on page 387.
New > Monitor	Opens the New Monitor window which enables you to define a new SiteScope monitor. For user interface details, see "New Monitor Dialog Box" on page 444.
Paste	Pastes monitors and monitor groups into the Health container.
Recreate missing health monitors	Enables you to restore health monitors that have been deleted from the **Health** container.
Reports	Enables you to select the type of SiteScope report you want to define. For details on this topic, see "SiteScope Reports" on page 1501.
Run Monitors	Runs the health monitors and opens an information window with the results.

Remote Server Tree

The monitor tree represents the remote servers configured in your network environment. The Shortcut Menu Options include descriptions of the context menu options available for each object in the remote server tree.

To access	Select the **Remote Servers** context. The remote server tree is displayed in the left pane.
See also	➤ "Working with Remote Servers" on page 583 ➤ "Remote Server Properties Page" on page 600

Remote Server Tree Objects

User interface elements are described below:

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

Remote Servers Shortcut Menu Options

User interface elements are described below:

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

Remote Server Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Copy to Template	Copies the remote server to a template group. For details on this topic, see "How to Create a Template by Copying Existing Configurations" on page 973.
Delete	Deletes the remote server
Detailed Test	Enables you to test the running commands on the remote host and check the permissions for the defined user. Available for UNIX servers only.
Test	Enables you to test the connection to the remote server.

Template Tree

The monitor tree represents the SiteScope solution template sets, template examples, Monitor Deployment Wizard templates, and user-defined templates that are available for deployment to monitor groups. The Shortcut Menu Options include descriptions of the context menu options available for each object in the template tree.

To access	Select the **Templates** context. The template tree is displayed in the left pane.
See also	➤ "SiteScope Templates" on page 943 ➤ "SiteScope Solution Templates" on page 1083 ➤ "SiteScope Templates Page" on page 977 ➤ "Templates Tree - Alerts Tab" on page 980

Template Tree Objects

User interface elements are described below:

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

UI Element	Description
	Represents a template configuration for deploying SiteScope objects. **Parent:** Template container. **Add to template tree by:** Creating.
	Represents a SiteScope template group or subgroup (with enabled monitors/with no monitors or no enabled monitors). If an alert has been set up for the template group or subgroup, the alert symbol is displayed next to the group icon. If a Management report has been set up for the template group or subgroup, the report symbol is displayed next to the group icon. **Parent:** Template. **Add to tree by:** Creating, or importing with a SiteScope that has template groups defined.
	Represents a SiteScope template monitor (enabled/disabled). If an alert has been set up for the template monitor, the alert symbol is displayed next to the monitor icon. If a Management report has been set up for the template monitor, the report symbol is displayed next to the monitor icon. **Parent:** Template group or subgroup, template, or solution template. **Add to tree by:** Creating, or importing with a SiteScope that has template monitors configured.

UI Element	Description
	Represents a Windows/UNIX remote server. **Parent:** Template. **Add by:** Creating in the remote server tree or template tree.
	Represents a variable used as placeholder to prompt for input when deploying a template. **Parent:** Template. **Add to template tree by:** Creating.

SiteScope Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Expand All	Opens all the subtrees under SiteScope.
Import	Opens the Import Template window which enables you to import a template file.
New > Template Container	Opens the New Template Container window which enables you to define a new template container.
Paste	Pastes a template container under the SiteScope root.

Solution Templates Container Shortcut Menu Options

User interface elements are described below:

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

Solution Template Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Copy	Copies a solution template. You can paste the solution template to a template container in the template tree.
Deploy Template	Opens the Select Group dialog box which enables you to select the group to which to deploy the solution template. For user interface details, see "Select Group Dialog Box" on page 1022.
Deploy Template Using CSV	Opens the Select Group dialog box which enables you to select the group to which to deploy the template using a CSV file. For user interface details, see "Select Group Dialog Box" on page 1022.
Expand All	Expands the solution templates container to display all the solution templates within the container.
Generate XML	Opens the Generate Auto Deployment XML window which enables you to create an XML file to use for automatically deploying the solution template. For details on the topic, see "Auto Template Deployment" on page 1053. For user interface details, see "Generate Auto Deployment XML User Interface" on page 1075.

Template Container Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Copy	Copies the template container and its contents. You can paste the template container under the SiteScope root or a selected template container in the template tree.
Cut	Moves the template container and its contents. You can paste the template container under the SiteScope root or a selected template container in the template tree.
Delete	Deletes the template container.

Menu Item (A-Z)	Description
Deploy Template	Opens the Select Group dialog box which enables you to select the group to which to deploy one or multiple templates. For user interface details, see "Select Group Dialog Box" on page 1022.
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.
Generate XML	Opens the Generate Auto Deployment XML window which enables you to create an XML file to use for automatically deploying the templates in the container.
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 or template container into the template container.

Template Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Copy	Copies the template and its contents. You can paste the template to a template container in the template tree.
Cut	Moves the template and its contents. You can paste the template to a template container in the template tree.
Delete	Deletes the template.
Deploy Template	Opens the Select Group dialog box which enables you to select the group to which to deploy the template. For user interface details, see "Select Group Dialog Box" on page 1022.
Deploy Template Using CSV	Opens the Select Group dialog box which enables you to select the group to which to deploy the template using a CSV file. For user interface details, see "Select Group Dialog Box" on page 1022.
Expand All	Opens all the subtrees under the template.
New > **Group**	Opens the New Group window, which enables you to define a new template group. For user interface details, see "New SiteScope Group Dialog Box" on page 387. **Note:** This menu item is available only if the template does not already contain a template group.
New > **UNIX Server**	Opens the New UNIX Remote Server window, which enables you to define a new remote UNIX template. **Note:** This menu item is available only if the template does not already contain a remote server.

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

Template Variable Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Copy	Copies the template variable. You can paste the template variable to a template in the template tree.
Cut	Moves the template variable. You can paste the template variable to a template in the template tree.
Delete	Deletes the template variable.

Template Remote Shortcut Menu Options

User interface elements are described below:

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

Template Group Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Copy	Copies the template group and its contents (monitors, alerts, and subgroups). You can paste the template group to a template in the template tree.
Cut	Moves the template group and its contents (monitors, alerts, and subgroups). You can paste the template group to a template in the template tree.
Delete	Deletes the template group.
Expand All	Opens all the subtrees under the template group.
New > Alert	Opens the New Alert window which enables you to define a new alert for the template group. For details on this topic, see "SiteScope Alerts" on page 1415.

Menu Item (A-Z)	Description
New > **Group**	Opens the New Group window which enables you to define a new template subgroup. For user interface details, see "New SiteScope Group Dialog Box" on page 387.
New > **Monitor**	Opens the New Monitor window which enables you to define a new SiteScope monitor for the template group. For user interface details, see "New Monitor Dialog Box" on page 444.
Paste	Pastes the selected template group and its contents (monitors, alerts, and subgroups) to a template.

Template Monitor Shortcut Menu Options

User interface elements are described below:

Menu Item (A-Z)	Description
Copy	Copies the template monitor and its contents (alerts). You can paste the template monitor to a template group in the template tree.
Cut	Moves the template monitor and its contents (alerts). You can paste the template monitor to a template group in the template tree.
Delete	Deletes the template monitor.
New > **Alert**	Opens the New Template Alert window which enables you to define a new alert for the template monitor. For details on this topic, see "SiteScope Alerts" on page 1415.
Paste	Pastes the selected template monitor and its contents (alerts) to a template group.

Preferences Menu

The Preferences menu represents the preference types that enable you to configure specific properties and settings related to most of the administrative tasks available within SiteScope.

To access	Select the **Preferences** context. The Preferences menu options are displayed in the left pane.
Important information	Only an administrator, or a user granted **Edit <preference type>** permissions, can create or make changes to SiteScope Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846.

User interface elements are described below:

UI Element	Description
<Preference types>	The following are the preference types in SiteScope: ➤ General Preferences. Use to perform post-configuration tasks, such as enter standard and optional SiteScope license keys, control display functions, and set security options. For details, see "General Preferences" on page 691. ➤ Infrastructure Preferences. Use to define the values of global settings that determine how SiteScope runs. For details, see "Infrastructure Preferences" on page 707. ➤ Integration Preferences. Use to configure SiteScope as a data collector for BSM. For details, see "Integration Preferences" on page 741. ➤ Log Preferences. Use to controls the accumulation and storage of monitor data logs. For details, see "Log Preferences" on page 783. ➤ Email Preferences. Use to define email server settings and profiles for SiteScope email alert and status reports. For details, see "Email Preferences" on page 791.

UI Element	Description
<Preference types> (continued)	➤ Pager Preferences. Use to configure settings and additional pager profiles that SiteScope uses for sending Pager alerts. For details, see "Pager Preferences" on page 801. ➤ SNMP Preferences. Use to define settings that are used by SiteScope SNMP Trap alerts when sending data to management consoles. For details, see "SNMP Preferences" on page 811. ➤ Common Event Mappings. Use to create event mapping instances between SiteScope runtime data and the event attribute values that are sent to the HPOM/BSM server. For details, see "Common Event Mappings" on page 819. ➤ Schedule Preferences. Use for customizing the operation of SiteScope monitors and alerts to run only at specific times or during specific time periods. For details, see "Schedule Preferences" on page 835. ➤ User Management Preferences. Use to define and manage user login profiles that control how others access SiteScope. For details, see "User Management Preferences" on page 845. ➤ Credential Preferences. Use to create and manage credentials for SiteScope resources. For details, see "Credential Preferences" on page 891. ➤ Search/Filter Tags. Use to manage the Search/Filter tags defined in SiteScope. You can assign tags to one or more items in the context trees and preference profiles, and then use the tags as an object for a filter. For details, see "Search/Filter Tags" on page 903. ➤ Certificate Management. Use to add and remove server certificates and reload the keystore, without having to restart SiteScope after each certificate change operation. For details, see "Certificate Management" on page 907.
<Preferences>	Represents a preference. Add by creating preferences in the specific preference container, or by importing a SiteScope that has preferences defined.

Server Statistics Menu

The Server Statistics menu enables you to view an overview of several key SiteScope server performance statistics. This includes the load on the SiteScope server, a list of currently running monitors and the most recently run monitors, perfex pool summary and statistics, WMI statistics, SSH connections, Telnet connections, and dynamic monitoring statistics. It also displays the SiteScope log files

To access	Select the **Server Statistics** context. The Server Statistics menu options are displayed in the left pane.
Important information	Only an administrator, or a user granted **View server statistics** permissions, can view the monitor performance data pages. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Analyze SiteScope Server Statistics" on page 1379
See also	"Using Server Statistics" on page 1372

User interface elements are described below:

UI Element	Description
<**Menu options**>	The following are the available monitor performance data options in SiteScope: ➤ **General.** Displays SiteScope server statistics, including the load on the SiteScope server (number of running monitors, waiting monitors, monitor runs per minute), and a list of running monitors by type. For details, see "General Page" on page 1393. ➤ **Running Monitors.** Displays a list of which SiteScope monitors are running, and which monitors have run recently, at what time, and what was the returned status. For details, see "Running Monitors Page" on page 1394. ➤ **Perfex Processes Pool.** Displays the process manager summary, and pool statistics and status tables for each pool. For details, see "Perfex Process Pool Page" on page 1396. ➤ **WMI Statistics.** Displays the process manager summary for Windows Management Instrumentation (WMI) statistics. For details, see "WMI Statistics Page" on page 1399. ➤ **SSH Connections.** Displays Secure Shell (SSH) statistics and a summary of SSH connections when using SSH to connect to remote UNIX or Windows servers. For details, see "SSH Connections Page" on page 1401. ➤ **Telnet Connections.** Displays telnet statistics when using telnet to connect to remote UNIX or Windows servers. For details of the user interface, see "Telnet Connections Page" on page 1403. ➤ **Dynamic Monitoring Statistics.** Displays statistics when using the dynamic monitoring mechanism to automatically update dynamic monitoring counters and thresholds. For details of the user interface, see "Dynamic Monitoring Page" on page 1405. ➤ **Log Files.** Displays the list of log files in SiteScope that are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions. For details of the user interface, see "Log Files Page" on page 1409.

Tools Menu

The Tools menu displays a list of diagnostic tools that can help you troubleshoot problems in SiteScope and facilitate monitor configuration.

To access	Select the **Tools** context. The Tools menu options are displayed in the left pane.
Important information	➤ To view or use the tools in the **Tools** context in the left pane, you must be an administrator in SiteScope, or a user granted **Use tools** permissions. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ Some tools are also available when configuring or editing specific monitors (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions). If a tool is available when configuring or editing a monitor, you can access the tool by: ➤ Clicking the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ Clicking the **Tools**  button in the SiteScope Dashboard toolbar when running the test tool for an existing monitor. This opens and runs the tool with the monitor's existing data as its input, and displays test results in the **Results** pane. ➤ To avoid character set problems when the SiteScope client uses a multibyte locale different from the SiteScope server, set the value in the **master.config** file for the **_httpCharset** setting to **UTF-8**. By default, the **_httpCharset** value is empty, which means that the default server locale is used.
See also	"SiteScope Tools Overview" on page 160

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

UI Element	Description
Application Tools	
Microsoft Windows Media Player Tool	Tests Microsoft Windows Media Player streaming. For more information, see "Microsoft Windows Media Player Tool" on page 195.
News Server Tool	Checks whether a News Server is operational. For more information, see "News Server Tool" on page 198.
Real Media Player Tool	Tests Real Media Player streaming. For more information, see "Real Media Player Tool" on page 205.
Common Utility Tools	
Regular Expression Tool	Tests a regular expression for content matching against a sample of the content you want to monitor. For more information, see "Regular Expression Tool" on page 207.
XSL Transformation Tool	Tests custom XSL transformation of XML data to be monitored with the Browsable XML Monitor. For more information, see "XSL Transformation Tool" on page 233.
Log Analysis Tool	Analyze patterns in a log file and provides a list of all reoccurring patterns. Each pattern can be transferred into a regular expression that can be used in the Log File monitor. For more information, see "Log Analysis Tool" on page 187.
Database Tools	
Database Connection Tool	Checks connectivity and configuration of JDBC or ODBC database connections. For more information, see "Database Connection Tool" on page 169.
Database Information Tool	Retrieves and displays database server metadata such as product and driver version, SQL compatibility level information, and supported SQL functions. For more information, see "Database Information Tool" on page 173.

UI Element	Description
LDAP Authentication Status Tool	Tests an LDAP server by requesting a user authentication. For more information, see "LDAP Authentication Status Tool" on page 184.
Mail Tools	
Mail Round Trip Tool	Tests a mail server by sending and retrieving a test message. For more information, see "Mail Round Trip Tool" on page 191.
Network Tools	
DNS Tool	Tests a DNS server to verify that it can resolve a domain name. For more information, see "DNS Tool" on page 176.
Network Status Tool	Displays the server's network interface status and active connections. For more information, see "Network Status Tool" on page 197. **Note:** This tool is not supported on SiteScopes installed on UNIX platforms.
Ping Tool	Performs a round-trip Ping test across the network. For more information, see "Ping Tool" on page 201.
Trace Route Tool	Performs a traceroute from your server to another location. For more information, see "Trace Route Tool" on page 219.
Operating System Tools	
Event Log Tool	Displays portions of the Windows Event Log locally or on a remote server. For more information, see "Event Log Tool" on page 178. **Note:** This tool is not supported on SiteScopes installed on UNIX platforms.
Performance Counters Tool	Checks connectivity to and values in Win NT Performance Counter registries. For more information, see "Performance Counters Tool" on page 199. **Note:** This tool is not supported on SiteScopes installed on UNIX platforms.

UI Element	Description
Processes Tool	Shows a list of currently running processes either locally or on a remote server. For more information, see "Processes Tool" on page 203.
Services Tool	Shows a list of currently running Windows Services. For more information, see "Services Tool" on page 209. **Note:** This tool is not supported on SiteScopes installed on UNIX platforms.
SNMP Tools	
SNMP Browser Tool	Browses an SNMP MIB and displays available OIDs. For more information, see "SNMP Browser Tool" on page 212.
SNMP Tool	Performs a SNMP get command to a specified SNMP host to retrieve a list of OIDs. For more information, see "SNMP Tool" on page 215.
SNMP Trap Tool	Displays the log of SNMP Traps received by SiteScope from SNMP-enabled devices. For more information, see "SNMP Trap Tool" on page 217.
Web Tools	
FTP Tool	Checks the availability of an FTP server and whether a file can be retrieved. For more information, see "FTP Tool" on page 181.
URL Tool	Requests a URL from a server and prints the returned data. For more information, see "URL Tool" on page 221.
Web Service Tool	Tests the availability of SOAP enabled Web Services. For more information, see "Web Service Tool" on page 226.

Alerts Tab Shortcut Menu Options

The Alerts tab shortcut menu options include descriptions of the context menu options available for alerts.

To access	Select the **Monitors/Templates** context. The Alerts tab is displayed in the right pane.
Relevant tasks	"How to Configure an Alert" on page 1443
See also	"SiteScope Alerts" on page 1415

User interface elements are described below:

Menu Item (A-Z)	Description
Copy	Copies the alert to the selected location in the monitor tree. **Note:** Available for alerts in the **Alerts on Monitor/Group** table only.
Copy to other SiteScope	This menu item is available only through SAM Admin when there is more than one SiteScope connected to BSM. Copies the alert from another SiteScope to the selected location in the monitor tree.
Delete	Deletes the alert.
Disable Alert	Disables the alert.
Edit Alert	Opens an editing window for the alert, which enables you to edit its settings.
Enable Alert	Enables the alert.
New Alert	Opens the New Alert dialog box, which enables you to create a new alert definition. For details on how to perform this task, see "How to Configure an Alert" on page 1443. **Note:** Available for alerts in the **Alerts on Monitor/Group** table only.

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

Reports Tab Shortcut Menu Options

The Reports tab shortcut menu options include descriptions of the options available for Management reports in the monitor tree.

Description	Select the **Monitors** or **Templates** context. The Reports tab is displayed in the right pane.
Relevant tasks	"How to Create a Report" on page 1508
See also	"SiteScope Reports" on page 1501

User interface elements are described below:

Menu Item (A-Z)	Description
Clear Selection	Clears the selection.
Copy Report	Copies the report to the selected location in the monitor tree. **Note:** Available for reports in the **Reports on Monitor/Group** table only.
Create New Report	Enables you to select the type of SiteScope report you want to create. For details on this topic, see "SiteScope Report Types" on page 1504. **Note:** ➤ Available for reports in the **Reports on Monitor/Group** table only. ➤ Only Management reports are added to the Reports tab.
Delete Report	Deletes the report.
Edit Report	Opens an editing window for the report, which enables you to edit its settings.
Generate Report	Generates the report.
Paste Report	Pastes the selected report. **Note:** Available for reports in the **Reports on Monitor/Group** table only.
Select All	Selects all the listed reports.
Show All Descendant Reports	Displays all descendent reports of the selected node.
Show Child Reports	Displays only those reports that are direct children of the selected node.

4

Searching and Filtering SiteScope Objects

This chapter includes:

Concepts

Tasks

Reference

Concepts

Searching and Filtering SiteScope Objects Overview

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

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

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

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

For details on filters, see "Defining and Managing Filter Settings" on page 117.

For details on tags, see "Working with Search/Filter Tags" on page 118.

Defining and Managing Filter Settings

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

You can define filters by:

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

Note: To create a filter based on specific common properties, use Global Search and Replace. For details, see "Global Search and Replace" on page 131.

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

Working with Search/Filter Tags

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

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

Tags can also be used in alert templates using the <tag> attribute. Using the **<tag:[tagName]>** property, you can include values in the filter tag as parameters in alerts. This provides similar functionality to the custom properties mechanism that was removed in SiteScope 10.00.

For example, you have a tag named AppServer with value Apache assigned to a monitor, and you include <tag:AppServer> in the alert template configured for that monitor. If an alert is triggered, the new property is replaced with Apache in the alert text. For details on alert template properties, see "SiteScope Alert Template and Event Properties Directory" on page 1451.

Tasks

How to Create and Define a New Search/Filter Tag

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

This task includes the following steps:

- "Create a search/filter tag" on page 119
- "Assign search/filter tags to SiteScope tree elements" on page 119
- "Define a tag for a filter setting" on page 120

1 Create a search/filter tag

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

For user interface details, see "Search/Filter Tags" on page 484.

For task details on adding a tag, see "New/Edit Tag Dialog Box" on page 129.

2 Assign search/filter tags to SiteScope tree elements

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

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

For details on the objects in the monitor tree, see "Monitor Tree" on page 81.

For details on the objects in the template tree, see "Template Tree" on page 95.

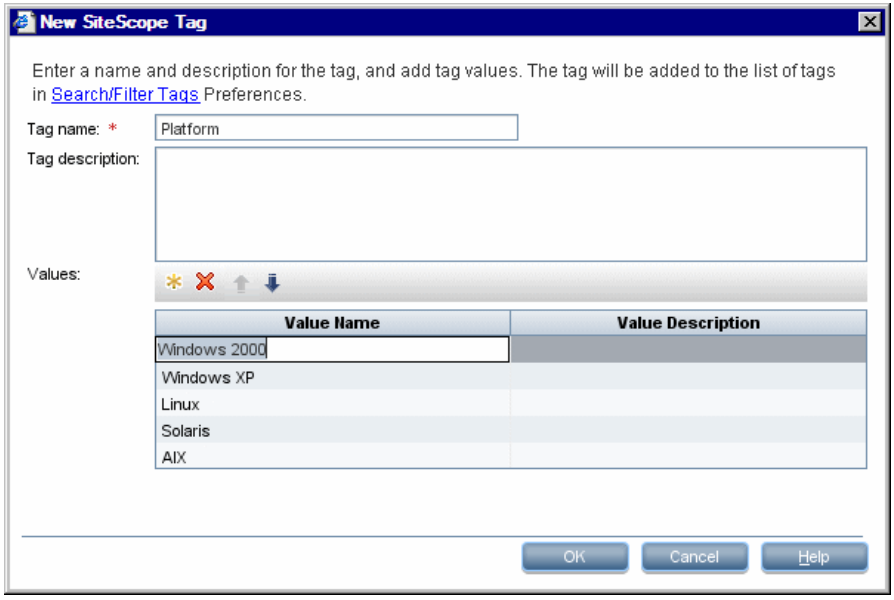
3 Define a tag for a filter setting

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

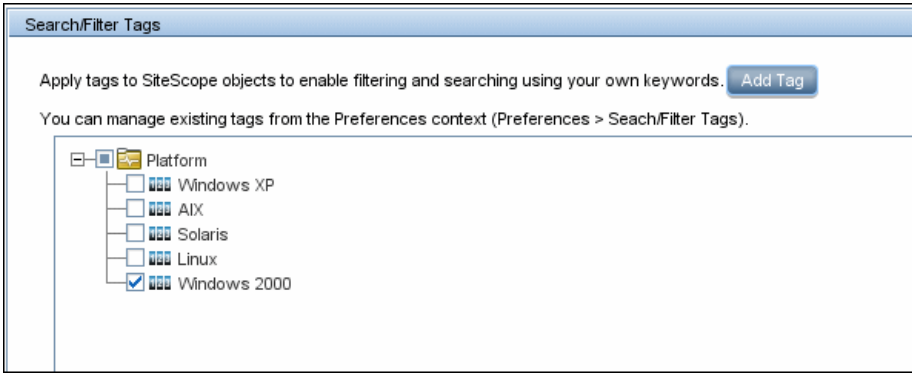
For details on filtering in the user interface, see "New/Edit Filter Dialog Box" on page 123.

Example:

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



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



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

Reference

Search/Filter Tags User Interface

This section includes (in alphabetical order):

New/Edit Filter Dialog Box

This dialog box enables you to add a new filter or edit an existing one when working in the monitor tree or the Manage Monitors and Groups dialog box.

To access	In the context toolbar (above the left tree pane), click the arrow next to the **Filter** button, and select **New Filter**, or select an existing filter and click **Edit**. After a filter has been applied, the filter icon is displayed as . The filter options are also available from the Manage Monitors and Groups dialog box.
See also	➤ "Searching and Filtering SiteScope Objects Overview" on page 116 ➤ "Defining and Managing Filter Settings" on page 117 ➤ "Tree Toolbar Buttons" on page 74

User interface elements are described below:

UI Element	Description
General Settings (This pane is not displayed when accessing the filter from the Manage Monitors and Groups dialog box)	
Filter name	Filter name. This name appears in the list of available filters when you click the **Filter** arrow.
Filter description	Description for the filter. This description appears only when editing the filter. **Note:** This field is optional.
Public filter	Describes the permissions of the filter. If the filter is public, all users can see, use, and edit the filter, but only the public filter owner can change this filter to a private filter. If the filter is not public, only the current user can see and use it.

UI Element	Description
Filter Options	
Regular expression	Enables using standard regular expressions to filter the monitor tree. When selected, you cannot select monitor names, monitor types, or tag values from the filter lists. The filter uses the POSIX regular expression format when the check box is cleared. **Default value:** Selected
Monitor name	To filter the objects appearing in the tree by the monitor name, type a monitor name. ➤ The monitor name is the string entered in the **Name** box in the General Settings area during monitor configuration. ➤ You can 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:** The expression /URL Monitor.* \.gov/ matches all monitor names containing the string URL Monitor with addresses containing the domain .gov. **Note:** This field is case sensitive.
Monitor type	To filter the objects appearing in the tree by the monitor type, enter the monitor type, or click the **Browse**  button and select the monitor types by which you want to filter in the Monitors list. For details on the Filter Monitor Types user interface, see "Filter Monitor Types Dialog Box" on page 126. **Note:** ➤ When entering multiple monitors, separate them with a comma (","). ➤ When entering a monitor type, you can enter a regular expression. **Example:** SAP* or CPU*

UI Element	Description
Target server	To filter the objects appearing in the tree by the target server, type a server name or click the **Browse** ... button and select the remote servers by which you want to filter from the Targets list. ➤ The target is the string entered in the **Server** box in the Monitor Settings area during monitor configuration. ➤ You can enter a regular expression to widen the filter. The tree displays only those monitors, within their groups, whose target server matches the string entered and only those groups containing these monitors. For details on the Filter Target Server user interface, see "Filter Target Servers Dialog Box" on page 127. **Note:** When entering multiple targets, separate them with a comma (",").
Tags	Enter tag values, or click the **Browse** ... button and select the tag values by which you want to filter in the Tags list. For details on the Filter Tags user interface, see "Filter Tags Dialog Box" on page 128. **Note:** ➤ When entering multiple tag values, separate them with a comma (","). ➤ You can use the wild card character ("*") and **or** expressions to filter tag values.
Enable/Disable monitor	Monitor status (enabled/disabled) by which you want to filter. **Default value**: None
HP BSM Logging	BSM logging option by which to filter. For details on the logging options, see "HP Integration Settings" on page 466.

Filter Monitor Types Dialog Box

This dialog box enables you to select the monitor type by which you can filter SiteScope objects.

To access	In the context toolbar, click the arrow next to the **Filter** button, and select **New Filter**, or select an existing filter and click **Edit**. In the New/Edit Filter dialog box, click the **Browse** button next to **Monitor Type**.
See also	➤ "Searching and Filtering SiteScope Objects Overview" on page 116 ➤ "Defining and Managing Filter Settings" on page 117 ➤ "New/Edit Filter Dialog Box" on page 123

User interface elements are described below:

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

Filter Target Servers Dialog Box

This dialog box enables you to filter SiteScope objects by the selected server targets configured in SiteScope.

To access	In the context toolbar, click the arrow next to the **Filter** button, and select **New Filter**, or select an existing filter and click **Edit**. In the New/Edit Filter dialog box, click the **Browse** button next to **Target Server**.
See also	➤ "Searching and Filtering SiteScope Objects Overview" on page 116 ➤ "Defining and Managing Filter Settings" on page 117 ➤ "New/Edit Filter Dialog Box" on page 123

User interface elements are described below:

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

Filter Tags Dialog Box

This dialog box enables you to select the tag values by which you can filter SiteScope objects.

To access	In the context toolbar, click the arrow next to the **Filter** button, and select **New Filter**, or select an existing filter and click **Edit**. In the New/Edit Filter dialog box, click the **Browse** button next to **Tags**.
See also	➤ "Searching and Filtering SiteScope Objects Overview" on page 116 ➤ "Defining and Managing Filter Settings" on page 117 ➤ "New/Edit Filter Dialog Box" on page 123

User interface elements are described below:

UI Element	Description
<Tag name and values>	Displays the tag names and tag values if tags have been created. Select the check box next to the tags that you want to include in the filter, and click **Save**. For concept details, see "Working with Search/Filter Tags" on page 118.

New/Edit Tag Dialog Box

This dialog box enables you to add a new search/filter tag.

To access	Select a SiteScope object (group, monitor, template, or preference profile), and open the **Search/Filter Tags** pane in the Properties tab or preference profile page. Click the **Add Tag** button.
Important information	➤ You can edit existing tags in the Preferences context (**Preferences** > **Search/Filter Tags**). For details on this topic, see "Search/Filter Tags Overview" on page 904. ➤ You cannot delete a Search/Filter tag or tag value if it is referenced by a SiteScope object. You must remove the tag or tag value from all SiteScope objects before you can delete it. ➤ Tags can also be used in alert templates using the <tag> attribute. For details, see "SiteScope Alert Template and Event Properties Directory" on page 1451.
Relevant tasks	"How to Create and Define a New Search/Filter Tag" on page 119
See also	"Working with Search/Filter Tags" on page 118

User interface elements are described below:

UI Element	Description
	**New.** Adds a tag value. A new row is added at the bottom of the list of tag values.
	**Delete.** Deletes the selected value from the tag.
	**Move up tag value.** Moves the selected tag value up the list of tag values. This enables you to sort the tag values order, instead of ordering alphabetically.
	**Move down tag value.** Moves the selected tag value down the list of tag values. This enables you to sort the tag values order, instead of ordering alphabetically.

UI Element	Description
Tag name	The name of the search/filter tag. **Maximum length:** 255 characters
Tag description	Description of the search/filter tag.
Values	Values included in the tag.
Value Name	Name for the value to be included in the tag. Each tag must include at least one value. Each value appears as a child object of the tag name when defining or editing tag settings for all objects in the monitor tree.
Value Description	Description for each value. This description appears only when editing the tag.

5

Global Search and Replace

This chapter includes:

Concepts

Tasks

Reference

Concepts

Global Search and Replace Overview

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

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

This section contains the following topics:

Filter Affected Objects

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

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

Replace or Find and Replace

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

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

Threshold Settings

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

- Have the same condition (**Error if**, **Warning if**, or **Good if**).
- Are configured for the same schedule.
- Use the same operator type (< <=, > >=, ==, !=, contains, !contains).

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

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

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

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

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

For details on setting thresholds, see "Setting Status Thresholds" on page 400.

Tasks

How to Perform a Global Search and Replace

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

This task includes the following steps:

1 Begin running the Global Search and Replace Wizard

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

For user interface details, see "Global Search and Replace Wizard" on page 142.

2 Select SiteScope (in SAM only)

Note: This step is only applicable when you access the Global Search and Replace wizard from SAM.

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

3 Select object type

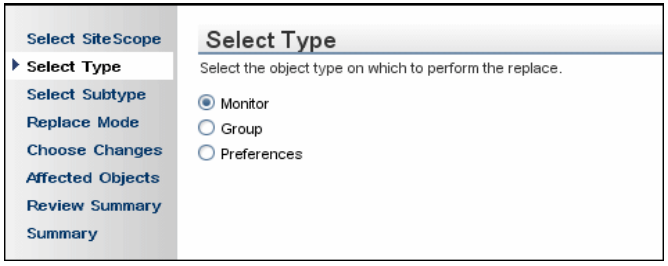
In the **Select Type** and **Select Subtype** page, select the object and, if relevant, the subtype on which you want to make a replacement.

For user interface details, see "Select Type Page" on page 144 and "Select Subtype Page" on page 145.

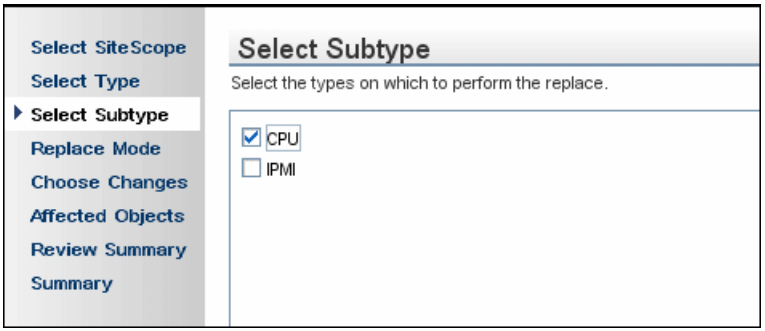
Example:

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

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



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



4 Search and replace objects

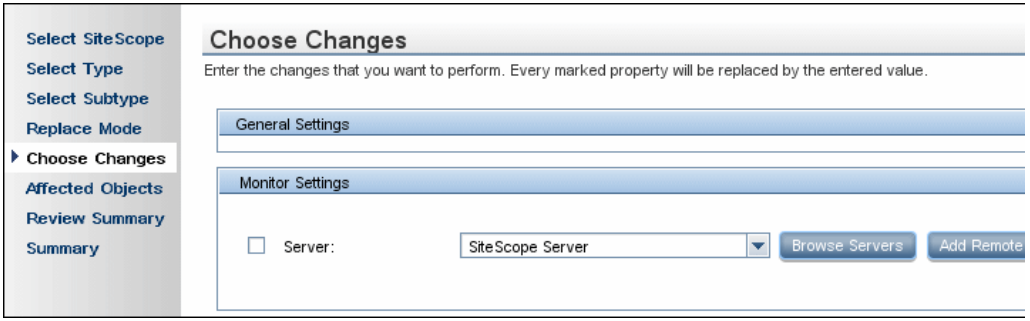
In the **Replace Mode** page, select the type of replacement. Select **Replace** to globally replace the object or select **Find and Replace** to replace specific instances of the object. Optionally, you can open the Advanced Filter dialog box to filter by the object properties. Here you select on which objects to perform the replace operation. In the **Choose Changes** page, you select what properties or values to replace.

For user interface details, see "Replace Mode Page" on page 145 and "Choose Changes Page" on page 147.

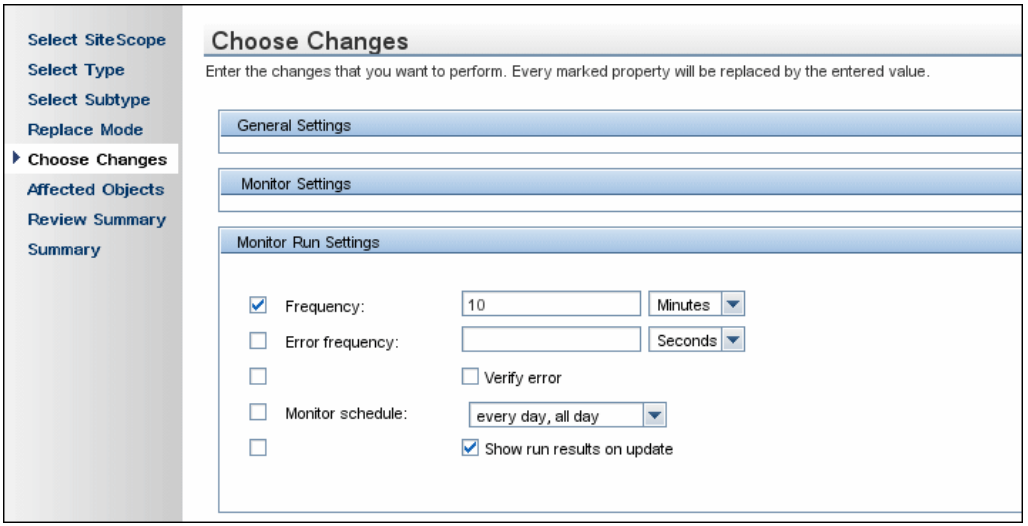
Example - Reducing the Frequency of a Monitor Run on a Specific Server:

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

You filter your selection in the Monitor Settings area in the Choose Changes page to include only those monitors monitoring the specified server.



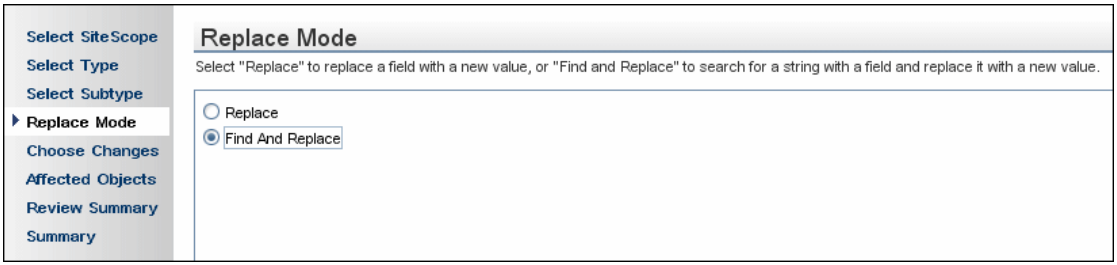
In the Choose Changes page, you then enter a new frequency of once a day, to monitor the specified server.



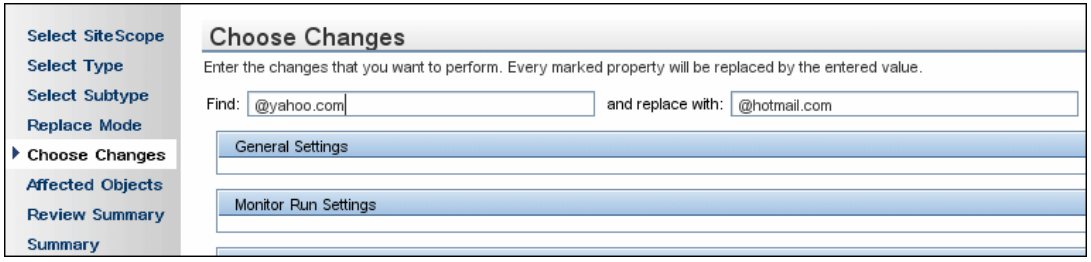
Example - Setting Up Alert Action to Send Alert Messages to Specified Email Addresses:

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

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



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



5 Check affected objects

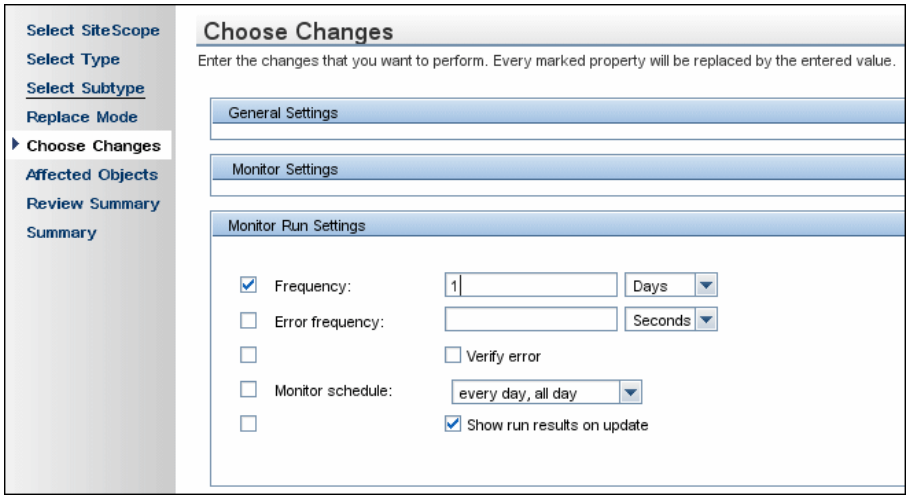
In the **Affected Objects** page, view the affected objects and, if necessary, clear or select objects for the replacement operation. Optionally, you can open the Filter Affected Objects dialog box to filter by the object properties. Here you select on which objects to perform the replace operation.

For user interface details, see "Affected Objects Page" on page 152.

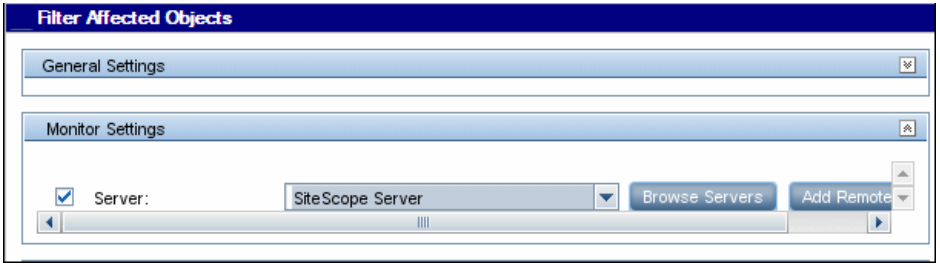
Example - Reducing the Frequency of a Monitor Run on a Specific Server:

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

If you had selected Replace in the Replace Mode page, in the Choose Changes page, you then enter a new frequency of once a day, to monitor the specified server.



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



6 Review replaced objects

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

For user interface details, see "Review Summary Page" on page 154 and "Summary Page" on page 156.

Reference

Global Search and Replace Wizard

This wizard enables you to make changes to group, monitor, preferences, alert, alert action, and report properties. These changes can be made across a SiteScope or across several SiteScopes when working in SAM Admin.

To access	➤ In SiteScope, right-click **SiteScope** root or the group or monitor in the monitor tree to which you want to perform the global replace. To replace Preferences objects, right-click **SiteScope** root. To replace alert objects, right-click **SiteScope** root, or the relevant group or monitor object. Select **Global Search and Replace** from the context menu. ➤ In BSM, select **Admin** > **System Availability Management.** Below the SiteScope Summary table in the right pane, click the **Global Search and Replace** button.
Relevant tasks	"How to Perform a Global Search and Replace" on page 135
Wizard map	This wizard contains: (Select SiteScope Page) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

Select SiteScope Page

Note: This page is displayed only when you are working in SAM Admin.

This wizard page enables you to select the SiteScope on which to make replacements.

Important information	➤ General information about this wizard is available here: "Global Search and Replace Wizard" on page 142. ➤ Only SiteScopes running version 9.0 and later and whose connection status permits configuration changes from SAM are listed. ➤ You must select at least one SiteScope.
Relevant tasks	"How to Perform a Global Search and Replace" on page 135
Wizard map	The Global Search and Replace Wizard contains: (**Select SiteScope Page**) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

Select Type Page

This wizard page enables you to select the object type on which you want to make replacements.

Important information	➤ General information about this wizard is available here: "Global Search and Replace Wizard" on page 142. ➤ Only those types of objects available for the node you selected are listed.
Relevant tasks	"How to Perform a Global Search and Replace" on page 135
Wizard map	The Global Search and Replace Wizard contains: (Select SiteScope Page) > **Select Type Page** > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

User interface elements are described below:

UI Element	Description
Alert **Alert Action** **Group** **Monitor** **Preferences** **Report**	You can select only one object type for each replace operation. Only those objects that exist in the SiteScope appear. When performing Global Search and Replace from SAM Admin, 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

This wizard page enables you to select the properties of the object type on which you want to make replacements.

Important information	➤ General information about this wizard is available here: "Global Search and Replace Wizard" on page 142. ➤ 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, Alert,** or **Report**, this page does not open.
Relevant tasks	"How to Perform a Global Search and Replace" on page 135
Wizard map	The Global Search and Replace Wizard contains: (Select SiteScope Page) > Select Type Page > **Select Subtype Page** > Replace Mode Page > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

Replace Mode Page

This wizard page enables you to select the type of replacement: global replacement or replacement based on filter criteria.

Important information	General information about this wizard is available here: "Global Search and Replace Wizard" on page 142.
Relevant tasks	"How to Perform a Global Search and Replace" on page 135
Wizard map	The Global Search and Replace Wizard contains: (Select SiteScope Page) > Select Type Page > Select Subtype Page > **Replace Mode Page** > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

User interface elements are described below:

UI Element	Description
Replace	Globally replaces all matching objects with the new string or value.
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**: ➤ If you select this option, only settings whose values can contain a string are available in the settings area of the **Choose Changes** page and can be selected for the find and replace action. ➤ 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.

Choose Changes Page

This wizard page enables you 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	➤ General information about this wizard is available here: "Global Search and Replace Wizard" on page 142. ➤ 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. ➤ The **Server** property is available only when monitors from the following group are selected: CPU, Disk Space, Memory, Microsoft Windows Performance Counter, Web Server, and Service monitor. For other monitors, the server attribute can only be changed by selecting that specific monitor subtype in the Select Subtype page. For example, if a CPU monitor is selected with a Web Server monitor, the server property is available. If a monitor not from this group is also selected, the server property is not available. ➤ **Note for users of SiteScope within SAM Admin**: If the SiteScopes selected for the replace operation are not all the same version, the subtypes of the SiteScopes may have different properties.
Relevant tasks	"How to Perform a Global Search and Replace" on page 135
Wizard map	The Global Search and Replace Wizard contains: (Select SiteScope Page) > Select Type Page > Select Subtype Page > Replace Mode Page > **Choose Changes Page** > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

User interface elements are described below:

UI Element	Description
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** box, enter the search string, value, or regular expression pattern for the setting or property you want to replace. ➤ In the **Replace With** box, enter the string or value to which you want all matching patterns to be changed. **Note:** If you select **Frequency** in the Monitor Run Settings, 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 appears. Reselect your filter criteria.
<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 select only the setting in the settings area. Enter the old and new values to replace in the **Find**/**Replace with** boxes. ➤ If you selected **Replace** in the Replace Mode page, you select the setting and the new value in the settings area. For details about some of the areas, see: ➤ "Threshold Settings Area" on page 149 ➤ "Filter Settings Area" on page 149 ➤ "Server Settings Area" on page 150

Threshold Settings Area

The **Threshold Settings** area is:

- Displayed only if you select **monitor** in the Select Type page, and one monitor in the Select Subtype page.
- Not displayed in the Choose Changes page, if you select more than one monitor in the Select Subtype page, and one of the monitors does not include threshold definitions.

The **Override Category** option is displayed in the **Threshold Settings** area only if you selected **Monitor** in the Select Type page:

- When the option is selected, you can override the threshold settings of the same threshold condition (**Error if**, **Warning if**, or **Good if**) for the selected monitor instances with the settings you enter here for the replace operation.
- When the option is cleared, the settings you enter here replace only those settings with the same operator type (< <=, > >=, !=, ==, contains, doesNotContain)) and the same configured schedule for the monitor instances. Any other settings for the same condition but with a different operator type or a different schedule remain. For details on this option and an example, see "Threshold Settings" on page 133.

Filter Settings Area

If you selected **Alert** in the Select Type page, the **Monitor type match** field in the Filter Settings is not displayed and its values cannot be replaced in the wizard.

Server Settings Area

The Server Settings area is displayed in the Choose Changes page if you select monitor in the Select Type page, and one monitor in the Select Subtype page.

If you select two or more monitors in the Select Subtype page, and these monitors do not belong to the same family (as listed in the table below), the Server Settings Panel is not displayed.

Family of Monitors	Monitors
SAP monitors	SAP Java Web Application Server SAP CCMS SAP CCMS Alerts SAP Performance SAP Work Processes
SNMP monitors	Cisco F5 Big-IP Network Bandwidth SNMP by MIB
URL monitors	URL URL List URL Content URL Sequence
Media Player monitors	Real Media Player Microsoft Windows Media Player

Family of Monitors	Monitors
Windows Counters monitors	ASP Citrix ColdFusion Microsoft Hyper-V Microsoft IIS Server Microsoft SQL Server Microsoft Windows Media Real Monitor
Server monitors	CPU Disk Space Memory Microsoft Windows Performance Counter Service UNIX Resources Web Server

Affected Objects Page

This wizard page enables you 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.

Important information	➤ General information about this wizard is available here: "Global Search and Replace Wizard" on page 142. ➤ The objects displayed depend on whether the user has change permissions on those objects. ➤ In SAM Admin, the permissions are set in BSM's Permissions Management (**Admin** > **Platform** > **Users and Permissions**). ➤ In SiteScope standalone, the permissions are set in **Preferences** > **User Management Preferences**. ➤ 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.
Relevant tasks	"How to Perform a Global Search and Replace" on page 135
Wizard map	The Global Search and Replace Wizard contains: (Select SiteScope Page) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > **Affected Objects Page** > (Filter Affected Objects Dialog Box) > Review Summary Page > Summary Page.

User interface elements are described below:

UI Element	Description
	**Filter.** Optionally, click to open the dialog box if you want to further refine your selections. For user interface details, see "Filter Affected Objects Dialog Box" on page 153.
<Affected Objects tree>	The Affected Objects tree includes all objects that are matched against the filter criteria selected in the previous pages of the wizard. Select or clear objects as required for the replace operation. **Note**: When using Global Search and Replace from SAM Admin, a tree is displayed for each SiteScope selected.

Filter Affected Objects Dialog Box

This dialog box enables you to select objects based on their specific settings and not only based on object type. For example, you can select all alerts that have a defined category of critical and replace any setting for those alerts. You can also select all groups with a dependency set to a specific monitor or group and replace any setting for those groups.

To access	Click the **Filter**  button in the Affected Objects Page.
Important information	➤ General information about this wizard is available here: "Global Search and Replace Wizard" on page 142. ➤ Using this option only refines your selection for the replace and does not determine what to replace.
Relevant tasks	"How to Perform a Global Search and Replace" on page 135
Wizard map	The Global Search and Replace Wizard contains: (Select SiteScope Page) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > (**Filter Affected Objects Dialog Box**) > Review Summary Page > Summary Page.

User interface elements are described below:

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

Review Summary Page

This wizard page enables you to preview the objects on which the replacement operation is performed. When working with multiple SiteScopes in SAM Admin, a table is displayed for each SiteScope and the name of the SiteScope appears above the table.

Important information	➤ General information about this wizard is available here: "Global Search and Replace Wizard" on page 142. ➤ 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 **Apply** in this page, you cannot undo the replacement operation.
Relevant tasks	"How to Perform a Global Search and Replace" on page 135
Wizard map	The Global Search and Replace Wizard contains: (Select SiteScope Page) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > **Review Summary Page** > Summary Page.

User interface elements are described below:

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

Summary Page

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 SAM Admin, a table is displayed for each SiteScope and the name of the SiteScope appears at the top of the table.

Important information	➤ General information about this wizard is available here: "Global Search and Replace Wizard" on page 142. ➤ There is no way to undo changes made by the replace operation. ➤ 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.
Relevant tasks	"How to Perform a Global Search and Replace" on page 135
Wizard map	The Global Search and Replace Wizard contains: (Select SiteScope Page) > Select Type Page > Select Subtype Page > Replace Mode Page > Choose Changes Page > Affected Objects Page > (Filter Affected Objects Dialog Box) > Review Summary Page > **Summary Page**.

User interface elements are described below:

UI Element	Description
	Change the sort order in the columns by clicking the up and down arrow in the column title. **Default:** The **Full Name** column is in alphabetical order, from top to bottom.
Full Name	Displays a tree of the server name, group, monitor name, and the monitor's properties whose value is being replaced.
<property>	The box name that you marked in the Choose Changes page that changes as a result of the replace operation.
Previous Value	The value that was replaced in the global replace operation.
New Value	The new value that resulted from the global replace operation.
	**Print.** Click to print the table. This icon appears for each table in the summary.
Apply	Closes the wizard.

6

SiteScope Tools

This chapter includes:

Concepts

Tasks

Reference

Concepts

SiteScope Tools Overview

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

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

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

For the list of SiteScope tools that are available, see "Tools Menu" on page 108.

User Permissions

The following permissions are required to use the SiteScope tools:

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

Tasks

How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor

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

This task includes the following steps:

1 Prerequisites

- To view and use the tools in the Tools context in the left pane, you must be an administrator in SiteScope, or a user granted **Use tools** permissions.
- To use the tools that are available when configuring specific monitors, you must be an administrator in SiteScope, or a user granted **Use monitor tools** permissions.

2 Add and configure a monitor

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

3 Configure and run the test

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

4 Apply the tested data to the monitor fields

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

5 Use a tool to edit or test monitor properties - optional

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

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

How to Use the Log Analysis Tool When Configuring or Troubleshooting a Log File Monitor – Use-Case Scenario

This task describes the steps involved in using the Log Analysis Tool when you want to configure a Log File monitor.

The administrator wants to create a Log File monitor for the most common problems or situations that are described in the log to be monitored. Once he selects the situation and creates the corresponding Log File monitor, the monitor runs as soon as a line corresponding to the selected situation is added to the log.

This task includes the following steps:

1 Prerequisites

- To view and use the tool in the Tools context in the left pane, the administrator must be an administrator in SiteScope, or a user granted **Use tools** permissions.
- To use the tools that are available when configuring specific monitors, the administrator must be an administrator in SiteScope, or a user granted **Use monitor tools** permissions.

2 Copy the log to analyze

The administrator copies the log he wants to analyze to the local SiteScope machine.

3 Run the Log Analysis Tool on that log

a The administrator selects **Tools** > **Common Utility Tools** > **Log Analysis Tool**.

b In the Log Analysis Tool dialog box, the administrator enters:

- **File location.** The location of the log copied to the local SiteScope server.
- **Message position.** The number of blocks (separated by blanks) that are to the left of the message to analyze for patterns.

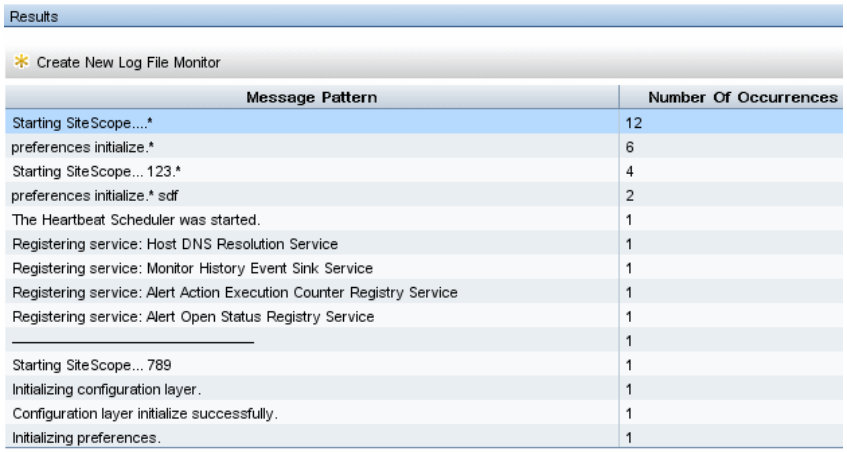
  For example, in the log structure that follows, the part of the log entry you are interested in is the message that starts after the 7th blank space (the space inside the date format is not included as it is part of the date format).

```
2010-11-02 11:49:02,738 [SiteScope Main Thread]
(SiteScopeHeartbeatManager.java:53) INFO  - The Heartbeat Scheduler was
started.
2010-11-02 11:49:02,786 [SiteScope Main Thread] (ServiceController.java:82)
INFO  - Registering service: Host DNS Resolution Service
```

- **Location of the date in the pattern.** The order of the block of text where the date is located. In the example above, the date is part of the first block of text.
- **Date Format.** In the example above, the date format follows the default. The default includes blanks.

➤ The administrator clicks **Run Tool**.

The Results box, in the Log Analysis Tool dialog box, displays the Regular Expression patterns found in the log and the number of instances of the pattern.


Results

Create New Log File Monitor

Message Pattern	Number Of Occurrences
Starting SiteScope....*	12
preferences initialize.*	6
Starting SiteScope... 123.*	4
preferences initialize.* sdf	2
The Heartbeat Scheduler was started.	1
Registering service: Host DNS Resolution Service	1
Registering service: Monitor History Event Sink Service	1
Registering service: Alert Action Execution Counter Registry Service	1
Registering service: Alert Open Status Registry Service	1
————————————	1
Starting SiteScope... 789	1
Initializing configuration layer.	1
Configuration layer initialize successfully.	1
Initializing preferences.	1

c The administrator selects the relevant pattern and clicks the **Create New Log File Monitor** button. In the Select group dialog box that opens, the administrator can select an existing group or create a new group by clicking the **New Group** button.

The **New Log File Monitor** dialog box opens, with the selected regular expression displayed in the **Content match** box.

d In that dialog box, the administrator enters the rest of the information needed to run the Log File monitor, including the path to the "real" log you want to analyze.

e The administrator clicks **Save** to save the new Log File monitor.

4 Results

The Log File monitor watches for specific entries added to the monitored log file that contain the selected regular expression. Depending on the monitor configuration, the administrator or the user can be notified of these conditions that you may have otherwise been unaware of until something more serious happened.

The new Log File monitor tool the administrator created is listed in the selected group in the monitor tree.

For details on the user interface, see "Log Analysis Tool" on page 187.

For details on the Log File monitor, see "Log File Monitor" in *Monitor Reference*.

Reference

SiteScope Tools User Interface

This section includes (in alphabetical order):

➤ URL Tool on page 221

➤ Web Service Tool on page 226

➤ XSL Transformation Tool on page 233

Database Connection Tool

This tool enables you 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 run and the results displayed.

➤ The database connection and resources can be closed.

This tool can be useful in verifying connection parameter values needed to set up database monitors, database alerts, and database logging.

To access	➤ Select **Tools** context > **Database Tools** > **Database Connection Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the Database Counter monitor, Database Query monitor, DB2 8.x and 9.x monitor, or Technology Database Integration monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.

Important information	➤ If exceptions or errors occur during the test, the information is printed along with suggested actions to help with troubleshooting. ➤ When using the Database Connection Tool to apply properties to the Database Query monitor or Technology Database Integration monitor, you must enter the credential data manually (if you select a credential profile the credential data is lost).
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Database connection URL	Database connection URL used when setting up the monitor. When using the Oracle thin driver, the database connection URL has the form of: jdbc:oracle:thin:@<server name or IP address>:<port>:<database sid>. **Example:** To connect to the ORCL database on a machine using port 1521, enter jdbc:oracle:thin:@206.168.191.19:1521:ORCL. The colon (:) symbol must be included as shown. For other examples of common database connection URLs, see the "Setup Requirements and User Permissions" section for the relevant database monitor. **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 **User Name** and **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	JDBC or ODBC driver that SiteScope should use. The .jar file or library containing the .class file must be installed in the <**SiteScope root directory**>**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. **Default value:** sun.jdbc.odbc.JdbcOdbcDriver **Example:** For examples of common database driver strings, see the "Setup Requirements and User Permissions" section for the relevant database monitor.

UI Element	Description
Credentials	Option for authorizing credentials if the database specified requires a name and password for access: ➤ **Use user name and password.** Select this option to manually enter user credentials. Enter the user name and password to access the database in the **User name** and **Password** box. ➤ **Select predefined credentials.** Select this option to have SiteScope automatically supply a predefined user name and password for the database (default option). Select the credential profile to use from the **Credential profile** drop-down list, or click **Add Credentials** and create a new credential profile. For details on how to perform this task, see "How to Configure Credential Preferences" on page 895.
Query	(Optional) SQL query to run on the database. If you do not supply a SQL query string, the driver is loaded and the connection to the database is tested but no query is run.
Result set maximum columns	Maximum number of columns to display in the query result set if you entered a SQL Query. **Default value:** 10
Result set maximum rows	Maximum number of rows to display in the query result set if you entered a SQL Query. **Default value:** 10
Run Tool	Runs the connection test. Connection results are displayed in the Results pane.
Save to File	Saves the results to a file.

Example

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

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

Database Information Tool

This tool enables you to view database server metadata such as product and driver version, SQL compatibility level information, and supported SQL functions.

To access	Select **Tools** context > **Database Tools** > **Database Information Tool** (you must have **Use tools** permissions)
Important information	Different database drivers and user names can significantly change what information is displayed.
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Database connection URL	Database connection URL used when setting up the monitor. When using the Oracle thin driver, the database connection URL has the form of: jdbc:oracle:thin:@<server name or IP address>:<port>:<database sid>. **Example:** To connect to the ORCL database on a machine using port 1521, enter jdbc:oracle:thin:@206.168.191.19:1521:ORCL. The colon (:) and the (@) symbols must be included as shown. For other examples of common database connection URLs, see the "Setup Requirements and User Permissions" section for the relevant database monitor.
Database driver	JDBC or ODBC driver that SiteScope should use. The .jar file or library containing the .class file must be installed in the **<SiteScope root directory>\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. **Default value:** sun.jdbc.odbc.JdbcOdbcDriver **Example:** For examples of common database driver strings, see the "Setup Requirements and User Permissions" section for the relevant database monitor.

UI Element	Description
Credentials	Option for authorizing credentials if the database specified requires a name and password for access: ➤ **Use user name and password.** Select this option to manually enter user credentials. Enter the user name and password to access the database in the **User name** and **Password** box. ➤ **Select predefined credentials.** Select this option to have SiteScope automatically supply a predefined user name and password for the database (default option). Select the credential profile to use from the **Credential profile** drop-down list, or click **Add Credentials** and create a new credential profile. For details on how to perform this task, see "How to Configure Credential Preferences" on page 895.
Run Tool	Runs the tool and displays database information. Test results are displayed in the Results pane.
Save to File	Saves the results to a file.

DNS Tool

This tool enables you to look up names from a Domain Name Server and show you the IP address for a domain name. It also shows you information about the name servers for a domain.

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 can look up the addresses for external domains.

To access	➤ Select **Tools** context > **Network Tools** > **DNS Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the DNS monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
DNS server	IP address or host name of a DNS server. If left empty, the local DNS server is used.
Host name to resolve	Domain name that you want translated into an IP address.
Run Tool	Runs the test. The tool sends the request to the DNS server entered in the **DNS server** box and displays the IP address for the host name entered in the **Host name to resolve** box. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

Event Log Tool

This tool enables you to view portions of the Windows event log locally or on a remote server.

To access	➤ Select **Tools** context > **Operating System Tools** > **Event Log Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the Microsoft Windows Event Log monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Important information	➤ Different database drivers and user names can significantly change what information is displayed. ➤ This tool is not supported on SiteScopes installed on UNIX platforms.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Server	The server on which you want to monitor event logs. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the **Browse Servers** button to select a server from the local domain, or **Add Remote Server** to add a new server. **Default value:** SiteScope Server (the server on which SiteScope is installed)
Browse Servers	Select the server to be monitored: ➤ **Browse servers.** Select a server from the drop-down list of servers visible in the local domain. ➤ **Enter server name.** If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. A double slash ("\ \") is automatically prefixed to any machine name supplied in the **Enter server name** box. **Note:** You must have domain privileges or authenticated access to the Windows remote server. For details on how to configure a remote Windows server, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.
Add Remote Server	Add and configure the remote server. For user interface details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603.

UI Element	Description
Log name	Select the type of log file you want to view: ➤ Application ➤ Directory Service ➤ DNS ➤ File Replication Service ➤ Security ➤ System **Default value:** System
Number of events displayed	Number of entries to list for this event log. The most recent entries in the log are displayed first. **Default value:** 10
Run Tool	Runs the test and refreshes the log entry listing. Log entries are displayed in the Results pane.
Save to File	Saves the results to a file.

FTP Tool

This tool enables you 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 access	➤ Select **Tools** context > **Web Tools** > **FTP Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the FTP monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Basic FTP Settings	
FTP server	IP address or the name of the FTP server that you want to test. **Example:** 206.168.191.22 or ftp.thiscompany.com
File	File name to retrieve. **Example:** /pub/docs/mydoc.txt
User name	Name used to log on to the FTP server.
Password	Password used to log on to the FTP server.
Passive mode	SiteScope uses a passive FTP connection. This is commonly required to access FTP servers through a firewall.
HTTP Proxy Settings	
HTTP proxy	Proxy name or IP address if you want to use a proxy server for the FTP test.
Proxy user name	Name used to log into the proxy server.
Proxy password	Password used to log into the proxy server.
Run Tool	Runs the test. Check The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

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

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

LDAP Authentication Status Tool

This tool enables you to verify that a Lightweight Directory Access Protocol (LDAP) server can authenticate a user by performing a simple authentication.

To access	➤ Select **Tools** context > **Database Tools** > **LDAP Authentication Status Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the LDAP monitor or Active Directory Replication monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

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

UI Element	Description
LDAP filter	Searches LDAP using the filter criteria. The LDAP filter syntax is a logical expression in prefix notation meaning that logical operator appears before its arguments. **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. **Example:** The filter syntax (& (sn=Freddie) (mail=*)) requests LDAP entries that have both a sn attribute of Freddie and a mail attribute.
Run Tool	Runs the test. LDAP Authentication test results are displayed in the Results pane.
Save to File	Saves the results to a file.

Log Analysis Tool

This tool enables you to search for patterns in a log. Once the tool has listed the patterns you can create a SiteScope Log File monitor to monitor that pattern in the log.

To access	Select **Tools** context > **Common Utility Tools** > **Log Analysis** (you must have **Use tools** permissions) **Note:** If you created a Log File monitor from this tool, the tool can also be accessed from the Log File Monitor (using the **Tools** button in the Dashboard toolbar).
Important information	➤ If the structure of the log you want to analyze is not consistent, you cannot use this tool. ➤ After you have created the Log File monitor for a pattern discovered by the Log Analysis Tool, the new monitor is listed in the monitor tree. ➤ To tell the Log Analysis Tool where the text you want to analyze is located in the log file, you can provide a regular expression or the number of blocks of text before the text you want to analyze. **Limitation:** The size of the log file you want to analyze should not be more than 10MB.
Relevant tasks	➤ "How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162 ➤ "How to Use the Log Analysis Tool When Configuring or Troubleshooting a Log File Monitor – Use-Case Scenario" on page 164
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Log Analysis Tool Area	
Folder location on SiteScope Server	Enter the path of the folder, on the SiteScope server, where the log file to be analyzed is located.

UI Element	Description
File name	Enter the name of the log file to be analyzed. You can enter a regular expression that matches the file names of the log files to be analyzed, when you want to analyze several files at the same time. **Example:** enter /error/ to analyze the error123.log and error345.log at the same time.
Use regular expression	To tell the Log Analysis Tool where the text you want to analyze is located in the log file, you can provide a regular expression or the number of blocks of text before the text you want to analyze. If you want to use the regular expression, select this option.
Regular expression	To tell the Log Analysis Tool where the text you want to analyze is located in the log file, you can provide a regular expression or the number of blocks of text before the text you want to analyze. This field is disabled when you clear the **Use regular expression** option. Enter the regular expression you want the tool to use to find the text you want to analyze between slashes (/). **Example:** For examples of regular expressions, see "Examples of Regular Expressions" on page 190.
Number of blocks before message	Log files include lots of information. The Log Analysis Tool is looking for patterns in the message (for example, the message after INFO or ERROR). This field is disabled when you select the **Use regular expression** option. To indicate to the tool where the message to analyze starts, you must specify the number of blocks of text (strings) separated by blank spaces that appear in each line of the log, before the start of the message you want to analyze. Ignore the blanks in the date if the date format includes blanks (see **Date format** below). **Note:** Logs that do not have a consistent structure cannot be analyzed by this tool.

UI Element	Description
Number of block where date is located	Enter the number of the block of text where the date is located counting from the left. The number of the first block is 1. This field is disabled when you select the **Use regular expression** option.
Date format	Select the date format used in the log. **Default format: yyyy-mm-dd HH:mm:ss,SSS**
Tool timeout (in seconds)	Amount of time, in seconds, to wait for the Log Analysis tool to run before timing out. **Default value:** 30 seconds
Run Tool	Runs the test. A list of all recurring message patterns is displayed in the Results box.
Results Area	
Create New Log File Monitor	Select a pattern and click the button to open the **Select group** dialog box where you can select a existing group or create a new group by clicking the **New Group** button. The **New Log File Monitor** dialog box opens, with the selected regular expression displayed in the **Content match** box.
Message Pattern	Displays a list of patterns found in the log. The list is ordered according to the number of occurrences of the patterns.
Number of Occurrences	Displays the number of instances of each pattern. The list is ordered according to the number of occurrences of the patterns.

Examples of Regular Expressions

Use the following regular expression:
\d*-\d*-\d*\s\d*.*,\d*\s\[\w.*\]\s\(\w.*\)\s\w.*\s\-\s
where **d** indicates a digit, **w** indicates a word, **s** indicates a space, and ***** indicates any character, for a log with the following structure:

```
2010-11-02 11:49:02,738 [SiteScope Main Thread]
(SiteScopeHeartbeatManager.java:53) INFO  - The Heartbeat Scheduler was started.
2010-11-02 11:49:02,786 [SiteScope Main Thread] (ServiceController.java:82) INFO  -
Registering service: Host DNS Resolution Service
2010-11-02 11:49:02,951 [SiteScope Main Thread] (ServiceController.java:82) INFO  -
Registering service: Monitor History Event Sink Service
2010-11-02 11:49:03,035 [SiteScope Main Thread] (ServiceController.java:82) INFO  -
Registering service: Alert Action Execution Counter Registry Service
2010-11-02 11:49:03,035 [SiteScope Main Thread] (ServiceController.java:82) ERROR
- Connection Error while trying to connect
2010-11-02 11:49:03,037 [SiteScope Main Thread] (ServiceController.java:82) INFO  -
Registering service: Alert Open Status Registry Service
2010-11-02 11:49:03,277 [SiteScope Main Thread] (SiteScopeSupport.java:655) INFO
```

Use the following regular expression:
\d*\s\w*\s\w*\s\d***\s\-\s** where **d** indicates a digit, **w** indicates a word, **s** indicates a space, and ***** indicates any character, for a log with the following structure:

```
123 Error starts *****12**** - The Heartbeat Scheduler was started.
123 Error starts *****23**** - Registering service: Host DNS Resolution Service
123 Error starts *****34**** - Registering service: Monitor History Event Sink Service
123 Error starts *****45**** - Registering service: Alert Action Execution Counter
Registry Service
123 Error starts *****45**** - Registering service: Alert Action Execution Counter
Registry Service
```

Mail Round Trip Tool

This tool enables you to check a Mail Server by using the network and verifies that the mail server is accepting requests and that a message can be sent and retrieved. It does this by sending a standard mail message using SMTP and then retrieving that same message by using a POP user account. Each message that SiteScope sends includes a unique key which it checks for to insure that it does not retrieve the wrong message and return a false OK reading.

To access	➤ Select **Tools** context > **Mail Tools** > **Mail Round Trip Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the Mail monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Basic Mail Settings	
Action	Select the action to take: ➤ **Send and receive.** Enables you to send a test message to an SMTP server and then receive it back from the POP3 or IMAP4 server to check that the mail server is up and running. (Default option) ➤ **Receive only.** 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. ➤ **Send only.** Checks that the receiving mail server has accepted the message.
Sending email server (SMTP)	Host name of the SMTP mail server to which the test mail message should be sent. **Example:** mail.thiscompany.com
Send to address	Mail address to which the test message should be sent.
Receiving protocol	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. **Default value:** POP3
Receiving email server	Host name of the POP mail server that should receive the test message. This can be the same mail server to which the test message was sent. **Example:** mail.thiscompany.com

UI Element	Description
Receiving email server user name	POP user account name. A test email message is sent to this account and the logs in to the account to verify that the message was received. No other mail in the account is touched. You can use your own personal mail account or another existing account for this purpose. **Note:** If you use an email reader that automatically retrieves and deletes messages from the server, there is a chance that the Mail Round Trip Tool never sees the mail message and reports an error.
Receiving email server password	Password, if necessary, for the test mail account.
Receive only content match	String of text to match against the contents of the incoming message. If the text is not contained in the incoming message, the Mail Round Trip reports an error. This is for the receiving only option (for example, Subject:MySubject). The search is case sensitive. 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.

UI Element	Description
Advanced Mail Settings	
Timeout (seconds)	Number of seconds to wait for a mail message to be received before timing-out. **Default value:** 300 seconds
POP check delay (seconds)	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. **Default value:** 10 seconds
NTLM authentication	NTLM version (version 1 or 2) if NTLM authentication is used by the email server. **Default value:** none
Show details	Displays details of the round trip test.
Run Tool	Runs the test. Check mail server test results are displayed in the Results pane.
Save to File	Saves the results to a file.

Microsoft Windows Media Player Tool

This tool enables you to test Microsoft Windows Media Player streaming.

To access	➤ Select **Tools** context > **Application Tools** > **Microsoft Windows Media Player Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the Microsoft Windows Media Player monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
URL	URL of the media file or streaming source you want to test. 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.
Duration (milliseconds)	Playback duration that the tool should use for the media file or source. The duration value does not need to match the duration of the media contained in the file. If the media content of the file or source you are testing is less than the duration value selected for the test, the monitor plays the entire media content and reports the results, including the time required to play the media content.
Run Tool	Runs the test. Check mail server test results are displayed in the Results pane.
Save to File	Saves the results to a file.

Network Status Tool

This 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 an increasing number of connections are being opened without being closed.

To access	Select **Tools** context > **Network Tools** > **Network Status Tool** (you must have **Use tools** permissions)
Important information	This tool is not supported on SiteScopes installed on UNIX platforms.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Run Tool	Runs the Network Status Tool and reports the network information. The data is displayed in the Results pane.
Save to File	Saves the results to a file.

News Server Tool

This tool enables you to access a News server and view the NNTP interaction between SiteScope (acting as a news client) and the News server.

To access	➤ Select **Tools** context > **Application Tools** > **News Server Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the News monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
News server	Name of the News server in the format news.sitescope.com or news.sitescope.com:7777.
News groups	(Optional) News group names. Separate multiple news group names by commas (",").
User name	User name if the News server specified above requires a name and password for access.
Password	Password if the News server specified above requires a name and password for access.

UI Element	Description
Run Tool	Runs the test. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

Performance Counters Tool

This tool enables you to check performance counters on a specific machine in a Windows NT/2000 network. It provides an interface to the **perfex.exe** executable supplied as part of SiteScope.

To access	➤ Select **Tools** context > **Operating System Tools** > **Performance Counters Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the CPU monitor, Disk Space monitor, Memory monitor, or Microsoft Windows Performance Counter monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Important information	This tool is not supported on SiteScopes installed on UNIX platforms.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Server	The server where the Windows performance counter objects you want to monitor are running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the **Browse Servers** button to select a server from the local domain, or **Add Microsoft Windows Remote Server** to add a new server. **Default value:** SiteScope Server (the server on which SiteScope is installed)
Browse Servers	Opens the Select Server dialog box, enabling you to select the server to be monitored: ➤ **Browse servers.** Select a server from the drop-down list of servers visible in the local domain. ➤ **Enter server name.** If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. A double slash ("\\") is automatically prefixed to any machine name supplied in the **Enter server name** box. **Note:** You must have domain privileges or authenticated access to the Windows remote server. For details on how to configure a remote Windows server, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.
Add Remote Server	Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details. For details on the Microsoft Windows Remote Servers user interface, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603. For details on the UNIX Remote Servers user interface, see "New/Edit UNIX Remote Server Dialog Box" on page 610.

UI Element	Description
Counters	Select a counter object to display the individual performance counters and corresponding values for the selected counter object.
Run Tool	Runs the tool and displays the individual Windows performance counters and corresponding values for the selected counter object. This information is displayed in the Results pane.
Save to File	Saves the results to a file.

Ping Tool

This tool displays the round trip time along a path. It sends a packet to another location and back to the sender. 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.

To access	➤ Select **Tools** context > **Network Tools** > **Ping Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the Ping monitor or Port monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.

Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Host name to resolve	Domain name or IP address of the host you want to ping. **Example:** demo.thiscompany.com or 206.168.112.53
Run Tool	Pings the domain name or IP address. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

Processes Tool

This tool displays processes running on the server where SiteScope is installed. This can be useful to confirm that critical processes are available.

To access	Select **Tools** context > **Operating System Tools** > **Processes Tool** (you must have **Use tools** permissions)
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Server	The server where the processes you want to monitor are running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the **Browse Servers** button to select a server from the local domain, or **Add Remote Server** to add a new server. **Default value:** SiteScope Server (the server on which SiteScope is installed)

UI Element	Description
Browse Servers	Opens the Select Server dialog box, enabling you to select the server to be monitored: ➤ **Browse servers.** Select a server from the drop-down list of servers visible in the local domain. ➤ **Enter server name.** If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. A double slash ("\\") is automatically prefixed to any machine name supplied in the **Enter server name** box. **Note:** You must have domain privileges or authenticated access to the Windows remote server. For details on how to configure a remote Windows server, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.
Add Remote Server	Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details. For details on the Microsoft Windows Remote Servers user interface, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603. For details on the UNIX Remote Servers user interface, see "New/Edit UNIX Remote Server Dialog Box" on page 610.
Run Tool	Runs the test. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

Real Media Player Tool

This tool enables you to test Real Media Player streaming.

To access	➤ Select **Tools** context > **Application Tools** > **Real Media Player Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the Real Media Player monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
URL	URL of the media file or streaming source you want to test. This should be the URL of the media file. **Note:** ➤ You can test video streams only (not audio) with this tool. ➤ This tool does not support metadata files such as the .smi format.
Duration (milliseconds)	Playback duration that the tool should use for the media file or source. The duration value does not need to match the duration of the media contained in the file. If the media content of the file or source you are testing is less than the duration value selected for the test, the monitor plays the entire media content and reports the results, including the time required to play the media content.
Run Tool	Runs the test. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

Regular Expression Tool

This tool enables you to perform a regular expression match.

To access	Select **Tools** context > **Common Utility Tools** > **Regular Expression Tool** (you must have **Use tools** permissions)
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Text	Copy and paste a portion of text containing the string or values on which you want to perform a regular expression match into this box. For efficiency in developing regular expressions, you should include all of the content that would precede the target data or pattern that you want to match. For example, when developing a regular expression for content matching on a Web page, you should use the URL Tool to retrieve the entire HTTP content including the HTTP header.
Regular expression	Enter a regular expression between the slashes //, to match some part of the text you entered. **Note:** 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. **Example:** /value:\W[\d]{2,6}/s
Run Tool	Runs the test. The results of the match test are displayed in the Results pane. If there is a problem with your regular expression, an error message is displayed.
Save to File	Saves the results to a file.

Parsed Parentheses and Matches Table

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

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

Services Tool

This 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.

To access	➤ Select **Tools** context > **Operating System Tools** > **Services Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the Service monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Important information	This tool is not supported on SiteScopes installed on UNIX platforms.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Server	The server where the services you want to monitor are running. Select a server from the server list (only those remote servers that have been configured in SiteScope are displayed). Alternatively, click the **Browse Servers** button to select a server from the local domain, or **Add Remote Server** to add a new server. **Default value:** SiteScope Server (the server on which SiteScope is installed)
Browse Servers	Opens the Select Server dialog box, enabling you to select the server to be monitored: ➤ **Browse servers.** Select a server from the drop-down list of servers visible in the local domain. ➤ **Enter server name.** If the server you want to monitor does not appear in the Servers list because it has not been identified in the network or has not been configured in Remote Servers, enter the IP address or name of the server to monitor. A double slash ("\\") is automatically prefixed to any machine name supplied in the **Enter server name** box. **Note:** You must have domain privileges or authenticated access to the Windows remote server. For details on how to configure a remote Windows server, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.
Add Remote Server	Opens the Add Remote Server dialog box, enabling you to select the type of remote you want to add (Windows or UNIX), and enter the configuration details. For details on the Microsoft Windows Remote Servers user interface, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603. For details on the UNIX Remote Servers user interface, see "New/Edit UNIX Remote Server Dialog Box" on page 610.

UI Element	Description
Run Tool	Runs the test. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

SNMP Browser Tool

This tool provides an XML representation of an SNMP agent's MIB. It can be used to verify the connection properties of an SNMP agent and to gain more information about the MIBs which that agent implements.

To access	➤ Select **Tools** context > **SNMP Tools** > **SNMP Browser Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the Cisco Works monitor, F5 Big-IP monitor, or SNMP by MIB monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Important information	➤ 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 an XML representation of the OIDs. Included in the XML tree are the textual and numeric names of the OIDs, their descriptions (if available), and their values at the time of traversal. ➤ The XML is displayed in a separate Results pane that displays lines numbers and highlights specific XML. If errors occur during the MIB traversal, an error message describing the problem is printed in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
SNMP Connection Settings	
Server	Host name or IP address of the device on which the SNMP agent is running that you want to monitor.
SNMP version	Version of SNMP which the tool should use when connecting to the agent. **Default value:** V1
Community	Community string to use when connecting to the SNMP agent for version 1 or 2 connections. **Default value:** public
Timeout (seconds)	Total time, in seconds, that SiteScope should wait for all SNMP requests (including retries) to complete. **Default value:** 5 seconds
Retries	Number of times each SNMP GET request should be retried before SiteScope considers the request to have failed. **Default value:** 1
Port	Port on which the SNMP agent is listening. **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 here. The default value is 1, which is commonly used and applicable to most applications. You should edit this box only when attempting to retrieve values from an application that does not handle OIDs starting with 1. If the default value of 1 did not enable retrieving any counters, then you may have to enter a different value.

UI Element	Description
MIB file	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. **Default value:** All MIBs
V3 SNMP Settings (This pane is enabled only if V3 is selected in the SNMP version field)	
SNMP V3 authentication type	The type of authentication to use for a version 3 connection. **Default value:** MD5
SNMP V3 user name	User name for a version 3 connection.
SNMP V3 authentication password	Password to use for authentication in a version 3 connection.
SNMP V3 privacy password	Password to use for DES privacy encryption in a version 3 connection. Leave this box blank if no privacy is desired.
SNMP V3 context engine ID	Hexidecimal string representing the Context Engine ID to use for this connection. This is applicable for SNMP V3 only.
SNMP V3 context name	Context Name to use for this connection. This is applicable for SNMP V3 only.
Run Tool	Runs the test. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

SNMP Tool

This tool lets you query a SNMP Management Information Base (MIB) and retrieve a set of OIDs.

To access	➤ Select **Tools** context > **SNMP Tools** > **SNMP Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the SNMP monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Host name	IP address of the server that hosts the SNMP MIB you want to query.
Object ID	ID of the next object that should be retrieved.
Index	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. **Example:** OID 1.3.6.1.2.1.2.2.1.17 is an indexed value that contains four elements. To access this second element of this OID, enter an index of 2 in this text box. **Default value:** 0
Community	Community string for the SNMP device. **Default value:** public
SNMP version	SNMP version used by the SNMP host you want to test. SiteScope supports both SNMP version 1 and version 2. **Default value:** V1
Number of records to get	Number of OID records to retrieve. **Default value:** 1
Run Tool	Runs the test. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

SNMP Trap Tool

This tool enables you to view SNMP Traps received by SiteScope's SNMP listener. The tool is only enabled if you have already created one or more SNMP Trap monitors. Creating an SNMP Trap Monitor enables the SiteScope SNMP Trap Log.

To access	➤ Select **Tools** context > **SNMP Tools** > **SNMP Trap Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the SNMP Trap monitor or Technology SNMP Trap Integration monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Important information	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.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Content match	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 SNMP Trap Log table title displayed in the lower part of the page.
Traps to show	Number of SNMP Traps to list. The number of traps is calculated, based on average trap length. If the trap text is longer or shorter than average, the number of traps shown can be different from the selected value. The most recent SNMP Traps received by SiteScope are displayed first. **Default value:** 10
Run Tool	Runs the test. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

Trace Route Tool

This tool 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.

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 access	Select **Tools** context > **Network Tools** > **Trace Route Tool** (you must have **Use tools** permissions)
Important information	You can use this tool to perform a traceroute on Windows platforms only. For UNIX, you must stop the SiteScope process, add the path of the traceroute utility (for example /usr/sbin/traceroute) to the **Traceroute command** box in Infrastructure Preferences, and then restart SiteScope.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Host name to resolve	Domain name or IP address of the other location to resolve. **Example:** demo.thiscompany.com or 206.168.112.53
Run Tool	Runs the test. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

URL Tool

This tool enables you 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.

To access	➤ Select **Tools** context > **Web Tools** > **URL Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the URL monitor, URL Content monitor, or Oracle 9i Application Server monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Main Settings	
URL	URL that you want to test. **Example:** http://demo.company.com
Match content	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").
Match content for error	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.
HTTP Settings	
URL content encoding	URL content encoding is the encoding in which the content is written. The encoding can be found in any of the following: ➤ HTTP headers: Content-Type: text/html; charset=UTF-8 ➤ HTML meta tag <meta http-equiv="Content-Type" content="text/html; charset=US-ASCII"> ➤ XML: <?xml version="1.0" encoding="ISO-8859-1"?> Select the encoding type from the drop down list. **Examples:** UTF-8, UTF-16, US-ASCII, ISO-8859-1 **Default value:** Encoding from server response
Retrieve images	SiteScope lists the images such as graphics, logos, and so on linked to the URL being requested.
Retrieve frames	SiteScope displays the HTML code of a frame linked to the URL being requested.

UI Element	Description
Authentication Settings	
Credentials	Option for authorizing credentials if the URL specified requires a name and password for access: ➤ **Use user name and password.** Select this option to manually enter user credentials. Enter the user name and password to access the URL in the **User name** and **Password** box. ➤ **Select predefined credentials.** Select this option to have SiteScope automatically supply a predefined user name and password for the URL (default option). Select the credential profile to use from the **Credential profile** drop-down list, or click **Add Credentials** and create a new credential profile. For details on how to perform this task, see "How to Configure Credential Preferences" on page 895.

UI Element	Description
Pre-emptive authorization	Option for sending authorization credentials if SiteScope requests the target URL: ➤ **Use global preference.** Select to have SiteScope use the setting specified in the **Pre-emptive 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 **User name** and **Password** entered for this monitor instance. If these are not specified for the individual monitor, the **Default authentication user name** and **Default authentication password** specified in the Main section of the General Preferences page are used, if they have been specified. **Note:** Pre-emptive authorization does not control if the user name and password should be sent, or which user name and password should be sent.
Client side certificate	The certificate file, if you need to use a client side certificate to access the target URL. Normally, this is a .pfx (.p12) type certificate, which usually requires a password. You enter the password for the certificate in the **Client side certificate password** box. **Note:** Client side certificate files must be copied into the <SiteScope root directory>\templates.certificates directory.
Client side certificate password	Password if you are using a client side certificate and that certificate requires a password.
Authorization NTLM domain	Domain for NT LAN Manager (NTLM) authorization if required to access the URL.

UI Element	Description
Accept untrusted certificates for HTTPS	If you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope does not have the required server certificates, you can either select this option or import the related certificates. For details on importing server certificates, see SSL Connectivity in "URL Monitor Overview" in the *Monitor Reference*.
Accept invalid certificates for HTTPS	Select this option if you are accessing a target URL using Secure HTTP (HTTPS) and SiteScope has invalid server certificates. This may happen, for example, if the current date is not in the date ranges specified in the certificate chain.
NTLM V2	Select if the URL you are accessing requires authentication using NTLM version 2.
Proxy Settings	
HTTP proxy	Address or domain name and port of an HTTP Proxy Server used to access the URL.
Proxy server user name	Name used to log on to the proxy server.
Proxy server password	Password used to log on to the proxy server.
Proxy NTLM V2	Proxy uses NTLM (Windows NT LAN Manager) version 2 to authenticate user logon.
Run Tool	Runs the test. The results of the test are displayed in the Results pane. The results include statistics on the URL retrieval as well as a text representation of the URL content.
Save to File	Saves the results to a file.

Web Service Tool

This tool enables you 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.

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.

To access	➤ Select **Tools** context > **Web Tools** > **Web Service Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the Web Service monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.

Important information	➤ 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. ➤ 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.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
WSDL Settings	
WSDL location	Select the WSDL location: ➤ **File.** Select the WSDL file to be used. This list reflects the files found by searching on **<SiteScope root directory>\templates.wsdl/*.wsdl**. Your WSDL files must have an extension of .wsdl. ➤ **URL.** Enter the URL of the Web service to be tested.
Get Data	Retrieves and analyzes the specified WSDL file for method arguments. The Result page displays the measurements available.
Service name	Name of the service to be invoked. During initial setup, this is extracted from the WSDL file.
Port name	Name of the port to be invoked. During initial setup, this is extracted from the WSDL file.
Method name	Name of the method to be invoked. During initial setup, this is extracted from the WSDL file.

UI Element	Description
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.

UI Element	Description
Name of arguments	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. **Example:** stockSymbol (string) = MERQ numShares (int) = 10 A complex type parameter must be represented as one long string (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> **Note:** 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.
Use user-defined SOAP XML	Use the XML in the **Use SOAP XML** box. This enables you to use XML that has been manually defined.
Use SOAP XML	Displays the SOAP XML for the selected Web service extracted from the WSDL file. You can make changes to the default XML, and use the manually defined XML in this box by selecting the **Use User-Defined SOAP XML** check box.

UI Element	Description
Main Settings	
Request's schema	The request schema. Currently SiteScope only supports SOAP.
Timeout (seconds)	Total time, in seconds, that SiteScope should wait for the Web service request to complete. **Default value:** 30 seconds
Use .NET SOAP	Select if the Web service is based on Microsoft .NET.
Content match	Text to check for in the returned page or frameset. If the text is not contained in the page, the tool displays the message no match on content. 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 Settings	
Web service server URL	Displays the URL of the Web service server to be checked.
HTTP user agent	HTTP user agent for the SOAP request.
HTTP content type	Content type of the HTTP request.

UI Element	Description
Proxy Settings	
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	User name if the proxy server requires a name and password to access the URL. **Note:** Your proxy server must support Proxy-Authentication for these options to function.
Proxy server password	Password if the proxy server requires a name and password to access the URL. **Note:** Your proxy server must support Proxy-Authentication for these options to function.
Login Settings	
NTLM domain	NTLM domain if the Web service requires NTLM / Challenge Response authentication as part of your credentials (as well as a user name and password below).
Authorization user name	User name if the Web service requires a user name and password for access (Basic, Digest, or NTLM authentication), enter the user name. Alternately, you can leave this entry blank and enter the user name in the **Default authentication user name** box on the General Preferences page. You use this alternate method to define common authentication credentials.
Authorization password	Password if the Web service requires a user name and password for access (Basic, Digest or NTLM authentication), type the password. Alternately, you can leave this entry blank and enter the password in the **Default authentication password** box on the General Preferences page. You use this alternate method to define common authentication credentials.

UI Element	Description
Run Tool	Runs the test. The results of the test are displayed in the Results pane. 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
Save to File	Saves the results to a file.

XSL Transformation Tool

This tool enables you to test a user-defined XSL file that can be used to transform an XML file or output. This might be a file from a Web application that contains performance metrics data. The use of an XSL transformation may be necessary to process XML data into an acceptable format for use by the browsable XML Monitor.

To access	➤ Select **Tools** context > **Common Utility Tools** > **XSL Transformation Tool** (you must have **Use tools** permissions) ➤ Also available when configuring or viewing the XML Metrics monitor (provided you are an administrator in SiteScope, or a user granted **Use monitor tools** permissions): ➤ Click the **Use Tool** button in the new monitor dialog box when configuring a new monitor, or in the monitor **Properties** tab when configuring an existing monitor. ➤ To run the test tool for an existing monitor, click the **Tools** button in the SiteScope Dashboard toolbar. This opens and runs the tool with the monitor's existing data as its input, and displays the test results in the Results pane.
Relevant tasks	"How to Use a SiteScope Tool When Configuring or Troubleshooting a Monitor" on page 162
See also	➤ "SiteScope Tools Overview" on page 160 ➤ "Tools Menu" on page 108

User interface elements are described below:

UI Element	Description
Main Settings	
XML URL	URL of the XML file that is the input for the transformation.
XSL file	Path to the XSL file you want to test. This path must be relative to SiteScope root folder. **Example:** <SiteScope root directory>\templates.applications\XmlApp1.xsl
Authentication Settings	
Authorization user name	User name needed to access the content if access to the target XML file requires authentication.
Authorization password	Password needed to access the content if access to the target XML file requires authentication.
Proxy server	Proxy server address if you are using a proxy server to access the target XML content.
Proxy server user name/password	User name and password required to use the proxy if you are using a proxy to access the target XML content.
Run Tool	Runs the test. The results of the test are displayed in the Results pane.
Save to File	Saves the results to a file.

7

Using Regular Expressions

This chapter includes:

Concepts

Reference

Concepts

Regular Expressions Overview

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

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

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

Defining a Regular Expression

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

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

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

- Create a regular expression using literal characters to match a single sample of the data you want to monitor. For example, /value: 1022.5/.
- Iteratively replace literal characters with character classes and metacharacters to generalize the literal into a pattern. For example, the literal in the example above could be changed to: /value:\s\d\d\d\d\.\d/ 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 enables variation in the number of digits to the left of the decimal point and the number of digits to the right of the decimal point. It expects that there is a decimal point. See the following sections for more information about the character classes used here.
- Consider that the literal string or pattern you want to match may appear more than once in the content. Identify unique content that precedes the content you want to match, and add regular expression patterns to make sure that the expression matches that unique content before it tries to match the content you are trying to monitor. In the example used here, the pattern may match the first of several entries that have a similar /value: numbers/ pattern. By adding a literal to the pattern that matches some static content that delimits the particular data can be used to be sure the match is made for the target data. For example, if the data you want to match is preceded by the text Open Queries, this literal can be added to the pattern, along with a pattern for any intervening content: /Open Queries[\s\W]{1,5} value:\s[\d]{1, 8}\.[\d]{1,2}/.

Matching String Literals

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

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

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

This section contains the following topics:

Example - Matching a Literal String

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

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

Reference

Matching Patterns with Metacharacters

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

This section contains the following topics:

Metacharacters Used in Regular Expressions

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 as opposed to the small \s which is used to match white space.

Metacharacter	Description
.	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.
\W	Matches characters other than those matched by \w (lowercase). 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 lowercase letters from a to z. You can also create more restrictive classes with the hyphen such as [e-tE-T] to match upper or lowercase 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 lowercase, 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, any white space, or both.
[\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 by using the browser. The HTTP header usually contains several lines of text including words coupled with sequences of numbers. This may cause failure of some otherwise simple content matching on short sets of numbers and letters. To avoid this, identify a unique sequence of characters near the text you are trying to match and include them as literals, where applicable, in the regular expression.

Search Mode Modifiers

Regular expressions used in SiteScope may include optional modifiers outside of the slashes used to delimit the expression. Modifiers after the ending slash affect the way the matching is performed. For example, regular expression of /website/i with the i search modifier added makes the match content search insensitive to upper and lowercase 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 lowercase 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 function to use content match values directly as thresholds for determining the error threshold of a URL monitor or URL Sequence monitor.

For example, if the content match expression was

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

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

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

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

```
2007
```

Under the error-if option at the bottom of the monitor set up page, you could then change the error-if condition from the default of status != 200 to content match, then specify the relational operator as !=, and then specify the value 2008. This sets the error threshold for this monitor so that whenever the year in the string Copyright is other than 2008, the monitor reports an error. This mechanism could be used to watch for unauthorized content changes on Web pages.

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

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

This expression matches the href="protocol://path/URLname.htm" for many URLs. The question mark modifiers enable the quotation marks around the HREF= attribute to be optional. The i modifier enables 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 date formats. The Language/Country Specific Date Variables enable you to automatically extend the language used for month names and weekday names to specific countries, based on ISO codes.

This section contains the following topics:

General Date Variables

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)
$monthName$	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 permitted for going backwards in time) before doing the substitutions.

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

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

the content string that would match would be:

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

Note: 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 paths for specific monitors. This is useful for monitoring date-coded files and directories where the URL or file path is updated automatically based on system date information. SiteScope is an example of an application that creates date-coded log files. The log file names include some form of the year, month, and day as part of the file name, such as File2001_05_01.log, where the year, month, and date are included.

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

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

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

the log file for the following day would be:

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

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

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

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

SiteScope monitor types that support the special substitution are:

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

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

Examples for Log File Monitoring

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

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

This section contains the following topics:

Searching Paths for Log Files

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

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

Example:

If you define the following path expression:

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

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

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

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

The monitor converts the characters between $L and $E to lowercase, /tmp/logs/arcv.log.tue.

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

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

the monitor converts the path to /tmp/logs/arcv.log.TUE.

You can use $L and $U multiple times in a path expression, and you can use them both in the same expression.

For example:

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

converts the path to /tmp/logs-tue/arcv.log.TUE

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

converts the path to /tmp.mar/logs-tue/arcv.log.TUE

Matching Comma-Separated Values

The following is an example of log file entries that are comma-separated strings of digits and letters:

```
new,open,changed,12,alerts
new,open,changed,13,alerts
new,open,changed,13,alerts
new,open,changed,14,alerts
```

A regular expression to match on log file entries that are comma-separated strings of digits and letters.

```
/([\w\d]+,[\w\d]+,[\w\d]+,[\w\d]+)[\n\r]?/
```

Note: If the file entries include punctuation marks such as an underscore or a colon, add that character explicitly to the [\w\d] class pattern. For example, to include a colon character, change each of the [\w\d] patterns to [\w\d:].

Matching Whitespace Separated Values

The following is an example of log file entries that are a sequence of strings and digits separated by spaces:

```
requests 12 succeeded 12 failed
requests 12 succeeded 12 failed
requests 11 succeeded 11 failed
requests 12 succeeded 12 failed
requests 10 succeeded 10 failed
```

The following is a regular expression to match on log file entries that are a sequence of strings and digits separated by spaces.

```
/([\w\d]+\s+[\w\d]+\s+[\w\d]+\s+[\w\d]+\s+[\w\d]+)[\n\r]?/
```

Note: The use of the + character forces the match to include the number of sequences per line included in the match pattern: in this example, five word or number sequences per line of the log file. If the sequences include punctuation marks such as an underscore or colon, add that character explicitly to the [\w\d] class pattern. For example, to include a colon character, change each of the [\w\d] patterns to [\w\d:].

Matching and Retaining the Numbers in a Line of Text and Numbers

The following is an example of log file entries that are comma separated strings that combine digits and letters:

```
request handle number 12.56, series 17.5, sequence reported 97.45, 15.95 and 19.51
request handle number 15.96, series 27.5, sequence reported 107.45, 25.95 and 19.52
request handle number 11.06, series 36.5, system codes 9.45, 35.95 and 19.53
log reference number 12.30, series 17.5, channel reset values 100.45, 45.95 and 19.54
```

The following is a regular expression to match on log file entries that are comma-separated strings that combine digits and letters and retain the decimal numeric data:

```
/[,\w\s]+(\d+\.\d+)[,\w\s]+(\d+\.\d+)[,\w\s]+(\d+\.\d+)[,\w\s]+(\d+\.\d+)[,\w\s]+(\d+\.\d+)[\n\r]
?/.
```

Note: If the file entries include punctuation marks such as an underscore or colon, add that character explicitly to the [,\w\s] class pattern. For example, to include a colon character that appears embedded in the text sequences, change each of the [,\w\s] patterns to [,:\w\s].

Matching Integers and Floating-point Numbers (Positive or Negative)

The following is an example of log file entries that are a sequence of integers and floating point numbers that may be negative or positive:

```
12.1987 -71 -199.1 145 -1.00716
13.2987 -72 -199.2 245 -1.00726
14.3987 -73 -199.3 345 -1.00736
15.4987 -74 -199.4 445 -1.00746
```

The following is a regular expression to match on log file entries that are a sequence of 5 integers and floating point numbers that may be negative or positive. The numbers in each entry must be separated by one or more spaces.

```
/(-?\d+\.?\d{0,})[\s]+(-?\d+\.?\d{0,})[\s]+(-?\d+\.?\d{0,})[\s]+(-?\d+\.?\d{0,})[\s]+(-
?\d+\.?\d{0,})[\n\r]?/
```

Matching Date and Time-Coded Log Entries

Many log files include some form of date and time data with each entry. The following is an example of log file entries that include date and time information together with string data separated by commas:

```
20/04/2003 14:29:22,ERROR,request failed
20/04/2003 14:31:09,INFO,system check complete
20/04/2003 14:35:46,INFO,new record created
```

The following is a regular expression to match on log file entries that are date- and time-coded followed by comma-separated strings of letters and digits. This example uses the SiteScope date variables to match only on entries that were created on the same day, month, and year as indicated by the system clock of the server where SiteScope is running.

```
/$0day$\/$0month$\/$year$\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]+)/
```

Problems Working with Regular Expressions

This section contains problems encountered when working with regular expressions.

This section contains the following topics:

Using the .* construct presents a very large number of possible matches on any page of content

The use of the .* construct is known to cause the regular expression-matching engine used by SiteScope to take over all available CPU cycles on the SiteScope server. If this occurs, SiteScope is unable to function and must be restarted each time the monitor with the offending regular expression is run, until the expression has been corrected.

Note: Regular expression matching is run against the entire text content returned to the SiteScope monitor request. This includes HTTP headers that are normally not viewable in the browser window (for example, not visible using the **View** > **Source** option). This also means that you must account for other information that may not be displayed in the browser view. This includes text in META tags used by Internet search engines as well as client side-scripts.

Text matching is done against code lines of the script (instead of against the browser's output from the script) for URLs containing client side-scripts, such as JavaScript

This means that if the script dynamically writes or replaces text on the Web page with values calculated by the script, it may not be possible to match this content with regular expressions. If the script is only changing text, you may be able to match the corresponding text strings that appear in the script code. A further pitfall would be that you are trying to check that a certain condition was met in the browser but the matching text string appears in the script content regardless of any user action.

Regular expression match succeeds as soon as the minimum match requested is satisfied

After a match is made, no further matching is performed. Therefore, regular expressions are not well suited to count the number of occurrences of a repeating text pattern. For example, if you want to check a Web page with a catalog list of items and each item has a link next to it saying Buy Now! and you want to make sure that at least five items are listed, a regular expression of /Buy Now!/ would succeed in matching only the first Buy Now!. Likewise, if your regular expression searches the word catalog on the main browser screen, the match may succeed if the word appears as a META tag in the HTML header section or if it appears as a hyperlink in a site navigation menu that appears in the content before the occurrence you intend to match.

Forgetting to account for non-alphanumeric content

Regular expressions need to be written to account for all of the characters that are and may be present. This includes white space, linefeed, and carriage returns. This is not normally a problem when matching a single-word literal. It can be a challenge when you need to create a match of several words separated by unknown amounts of white space and other non-alphanumeric characters and possibly span more than one line. The [\s\n\r]+ character class can be useful between words used in the expression. Always check the format of the content you are trying to match to look for patterns and special characters, such as periods, commas, and hyphens, that may cause a seemingly simple match to fail.

Use of excessive metacharacters can be problematic

In some cases, overly generous quantifiers combined with the . or \W metacharacters can grab content that you were intending to match with a literal string elsewhere in your regular expression resulting in a match failure. For example, the following might be used to match the URL content of the hyperlink anchor reference: /a href="([\W\w\s]*)"/. When the monitor performs the check for this regular expression, however, the match grabs the first occurrence of the pattern /a href="... and continues matching multiple lines of text up to the last quotation mark found on the page. Without some other unique ending delimiter, the [\W\w\s]* class and quantifier combination is too excessive. A more successful syntax that narrows the class of expected characters would be: /a href="?([:\/\w\s\d\.]*)"?/

Example Regular Expression Syntax

The following are some examples of syntax for use in regular expressions:

Example Expression	Description
/CUSTID\s?=\s?([A-Z0-9]{20,48})/	This example matches an ID string that is made of 20 or more digits and upper-case letters with no spaces or other non-alphanumeric characters. The \s? construct permits 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.

Part III

Integrations

8

Working with Business Service Management (BSM)

This chapter includes:

Concepts

Tasks

Reference

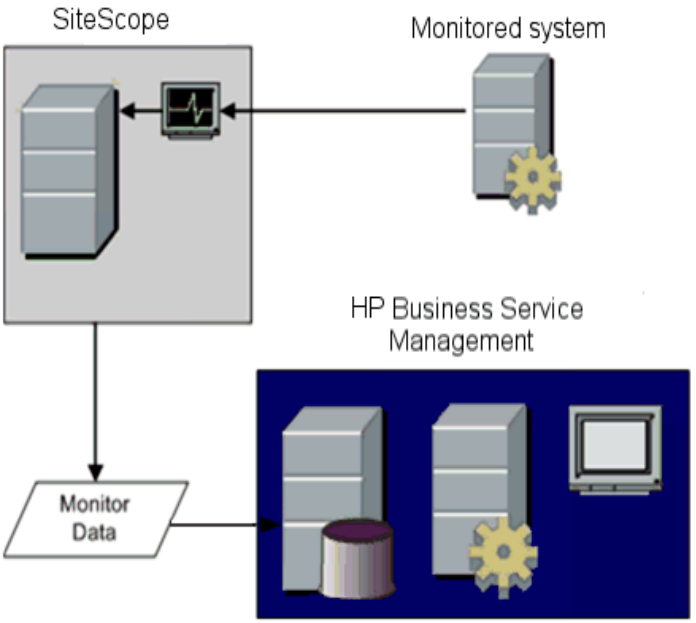
Concepts

Understanding How SiteScope Communicates with BSM

SiteScope can be used as a data collector for Business Service Management (BSM). BSM uses data about end-users, business processes, and systems.

When configured as a data collector to BSM, the metrics and topology data collected by SiteScope monitors can be passed on to BSM for analysis and for use in reports. Monitor data can be sent for all monitors or for selected monitors only.

The following diagram illustrates the use of SiteScope as a data collector for BSM.



Note: This integration should not be confused with metrics integration using the HP Operations agent, which is required to display metrics data in the Performance Perspective tab in Operations Management and in HPOM. For details on collecting metrics using the HP Operations agent, see "Reporting Metrics Using the HP Operations Agent" on page 322.

BSM includes a System Availability Management Administration page (SAM Admin), that enables you to manage SiteScope monitor configurations for one or more SiteScope servers through a central console. After activating the BSM integration, SiteScope data flows to BSM regardless of whether you manage SiteScopes through SAM Admin or the SiteScope standalone user interface.

For the BSM versions supported in this release, refer to the HP SiteScope Support Matrices section in the SiteScope release notes (in SiteScope, select **Help** > **What's New?**)

Tip: For best practices and troubleshooting for reporting metrics data to BSM and HPOM, see Best Practices for the SiteScope-BSM/OM Integration in the SiteScope Help.

Configuring the Connection

To enable the connection between SiteScope and BSM, the SiteScope must be configured as a data collector for BSM. This involves adding a SiteScope to the SAM Admin page in the BSM. For details on this task, see "How to Configure the Integration Between SiteScope and BSM" on page 288.

For details on configuring integration preferences, see "Integration Preferences Page" on page 757.

For information about troubleshooting reporting data to BSM, see "Troubleshooting and Limitations" on page 304.

Using SSL for SiteScope-BSM Communication

You can use Secure Sockets Layer (SSL) to transmit data from SiteScope to the BSM server. If you have installed a certificate signed by a root Certificate Authority on the BSM server, no additional setup is required on the SiteScope server.

If you are using a self-signed certificate on the BSM server and want to use that certificate for secure communication with SiteScope, you must perform the steps as described in "Configure SiteScope to connect to a BSM server that requires a client certificate or SSL - optional" on page 291.

Changing the Gateway Server to Which SiteScope Sends

You can change the Gateway Server to which a SiteScope reports its data. Generally, this is only applicable if you are working with a BSM deployment with components installed on more than one server (in the case of a distributed deployment where the BSM Gateway Server is installed on a different machine to the Data Processing Server).

For details on making this change, see "Change the Gateway Server to which SiteScope sends data - optional" on page 292.

Integrating SiteScope Data with BSM's Configuration Items

When a monitor instance is added to a SiteScope reporting data to BSM, that monitor creates a corresponding configuration item (CI) in the Run-time Service Model (RTSM). For details on understanding configuration items, see "Configuration Items (CI)" in the *RTSM Administration Guide* in the HP Business Service Management Documentation Library.

The SiteScope monitors that populate the RTSM include both actual monitors and the groups in which they are created.

- Actual monitors instances are represented in the RTSM as monitor CIs. Monitor CIs receive data from the corresponding SiteScope monitor instance and use the data, along with health indicators (HIs) and event type indicators (ETIs) that are assigned to SiteScope monitor metrics, to calculate key performance indicator status. These indicators provide a more detailed view of the health of a configuration item (CI). For details on understanding indicators, see "Health Indicators, KPIs, and KPI Domains" in *Service Health* in the HP Business Service Management Documentation Library.
- SiteScope groups are represented as group CIs in the RTSM and receive KPI status from the monitor CIs created by the monitors they are running.

Monitor Types and Topology Reporting

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

- **Technology Integration Monitors**. These monitors report data based on the topology settings script you select and edit for the monitor. The data they report is tightly integrated with BSM. You can create a custom topology or use a predefined script to forward the relevant data. For details on these monitors and how to work with their topology settings, see "Topology Settings for Technology Integration Monitors" on page 527.
- **Monitors of Supported Environments**. For these supported environments SiteScope acts like a discovery probe when the monitor is created or its configuration is changed. When topology reporting is enabled, SiteScope automatically discovers the application's topologies and populates the RTSM with the relevant CIs and monitor CIs. For details and a list of supported environments, see "Reporting Discovered Topologies to BSM" on page 282.

  You can create a custom topology for monitors of a supported environment (except for monitors where the CI type is per metric as described in "Monitors Reporting CI Per Metric" on page 303). For details on creating a topology, see "How to Configure Topology Reporting" on page 298.
- **Monitors Not Reporting Topology Data By Default.** SiteScope includes monitors that do not report hosts or servers and, therefore, it is not possible to know the CI type that is being monitored in advance. To include topology data for these monitors when reporting to BSM, you must select the CI type, define CI type key attributes, and map metrics related to the monitor type to specific indicators. SiteScope then creates a CI for the monitor in the RTSM and forwards monitor CI data to BSM. For the list of monitors that do not have a default topology defined, see "Monitors Not Reporting Topology Data By Default" on page 302.

This section also includes:

Creating Relationships Between Monitors and CIs

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

You can create these relationships in SiteScope or in SAM Admin. For details, see task step "Create relationships between SiteScope monitors and existing CIs in the RTSM - optional" on page 293.

Aging of CIs in the RTSM

In RTSM, CIs that have had no activity over a period of time are removed from the database. The CIs created from SiteScope data are also subject to this aging policy. To prevent the aging policy from acting on CIs that SiteScope has sent to BSM, SiteScope synchronizes the data it sends to BSM. The synchronization refreshes the data for those CIs and creates activity on the CIs.

For details on setting the time interval for topology synchronization, see "Topology Settings" in *Using System Availability Management* in the HP Business Service Management Documentation Library. For details on the aging mechanism, see "Working with CIs" in the *Modeling Guide* in the HP Business Service Management Documentation Library.

Note:

- Synthetic monitors and groups created by the EMS integration monitors that use Measurement field mapping are subject to the aging process regardless of the synchronization.
- To prevent CIs for EMS integration monitors being removed from the RTSM when aging is enabled, EMS topology is resent during a hard synchronization of SiteScope. In addition, you can enable topology resending as part of an anti-aging process by adding the property **_reportEmsCIsAsPartOfAntiAging=true** to the **master.config** file.
- If you delete a CI from RTSM you must perform a resynchronization or a hard synchronization of SiteScope (in Integration Preferences), or you must wait for a restart of SiteScope so the CI is restored to RTSM. This is due to the CI cache in SiteScope that prevents SiteScope from sending an unchanged CI twice. For details, see "BSM Preferences Available Operations" on page 764.

Managing Indicator Assignments in System Availability Management

---

Note: This section is relevant only to those users connecting SiteScope with BSM 9.00 or later.

SiteScope metrics that are mapped to indicators, are stored and managed in the Indicator Assignments repository in SAM Admin. The repository provides the following benefits:

- Centralized management of metric mappings in BSM, which makes it easier to manage large numbers of SiteScope and monitors. The Indicator Assignments repository is available for editing in the **Metrics and Indicators** tab in SAM Admin.
- Metrics are mapped from different SiteScope monitors to indicators, per monitor type. You can create, edit, and delete indicator assignments for specific monitor types.
- If new indicator assignments are added or existing assignments are modified in the Indicator Assignments repository, these changes can be published to all SiteScopes that are connected to BSM. This ensures that new monitor instances created in SiteScope have indicators according to the latest centralized assignments. You can restore the default assignments included in your current version of SiteScope by clicking the **Reset to Default** button in **HP Integration Settings** > **Indicator Settings** section of the monitor properties.

Note: Where indicator assignments have been modified on a local SiteScope server (mappings for monitor metrics were changed):

- These assignments are not overridden by the centralized assignments when SiteScope downloads the updated mappings.
- If an assignment is deleted from the Indicator Assignments repository, the local assignment is not automatically deleted and SiteScope keeps sending the old indicator value to BSM. In this case, a different indicator assignment should be selected for the monitor metric.
- If an indicator is deleted from the Indicator repository, a different indicator assignment should be selected for monitor metrics that used the mapping.

- The central repository ensures compatibility with earlier versions of SiteScope by mapping metrics from earlier SiteScopes to indicators.
- When a hard synchronization is performed on SiteScope, all the indicator mappings are downloaded from BSM.

For details on editing the centralized Indicator Assignments in SAM Admin, see "Indicator Assignment Settings" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

Assigning SiteScope Metrics to Indicators

Note: This section is relevant only to those users connecting SiteScope with BSM 9.00 or later.

When configuring monitor instances, you can also map a metric to an indicator. SiteScope monitor metrics are mapped to indicators on a monitor type basis as follows:

- Monitors of supported environments and monitors that have a defined topology have indicators assigned to metrics by default. For details of these monitors, see "Monitor Types and Topology Reporting" on page 274. For the list of default indicator assignments, see "Indicator Mapping Alignment" in *Using System Availability Management* in the HP Business Service Management Documentation Library.
- For SiteScope monitors that do not have a defined topology, there are no default indicator mappings, since these monitors can be linked to different CI types, and a single mapping cannot be set. For these monitors, you can map metrics to the appropriate indicators for the CI type linked to the monitor. For a list of monitors that do not have a defined topology, see "Monitors Not Reporting Topology Data By Default" on page 302.

You can change the default metrics mappings in SiteScope. If indicator mappings are modified locally in SiteScope, these mappings are not overridden by the centralized repository mappings when SiteScope downloads the latest mappings from BSM. This enables you to:

- Override indicators for a monitor instance or some metrics of a monitor.
- Configure non-default indicators in templates. Note that the CI type for custom topology and metric mappings is not configurable through variables in templates (they should be predefined in a template).

- Configure indicators for alerts. Since the CI type of a triggered alert is not always known when the alert is configured (for group alerts and alerts for Monitors Reporting CI Per Metric), you can manually enter the event type indicator and event type indicator state for an alert. For details, see "HP Operations Manager Integration Settings" on page 1468.

For details on mapping SiteScope metrics to indicators, see "Map Indicators to monitors" on page 300.

For user interface details, see "Indicator Settings" on page 472.

When are Health Indicators Created

- Events in SiteScope are based on SiteScope monitor metric status changes and alerts being triggered. Events are created after the first event arrives to the CI. For more details, see "Event Generation" on page 316.
- Metrics are created when the monitor topology is reported to the RTSM. For more details, see "Reporting Discovered Topologies to BSM" on page 282.

Discovery Scripts and the Package Manager

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

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

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

Note: Advanced users may want to modify the topology scripts within the package. Be warned that the **SiteScope** package uses scripts from other packages which may be shared by SiteScope and Data Flow Management. Any changes made to the scripts in the package can also affect Data Flow Management.

Any changes made to the topology script that influence the way a topology is reported to BSM can affect all the applications that use those topologies, including BSM applications and Operations Management.

Topology Reporting Limitation

The number of characters in SiteScope group and monitor descriptions that can be reported to BSM is limited to 600 characters. If a group or monitor description contain more than this number, SiteScope truncates the description to the first 600 characters.

Reporting Discovered Topologies to BSM

Note: This section is relevant only to those users connecting SiteScope with Business Availability Center/BSM 7.50 or later.

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

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

For details on the Topology Settings user interface, see "Topology Settings" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

For troubleshooting problems involving topology reporting, see "Business Service Management Topology Issues" in *Best Practices for the SiteScope-Business Service Management/Operations Manager Integration* in the SiteScope Help.

Supported Environments

This direct connection between SiteScope and BSM is available only for selected environments and with specific versions of BSM. SiteScope reports specific topologies for the following monitors:

Environment/ Monitor Type	Monitors
Monitors Reporting Node Topology	This includes all monitors that report the status of a host or server (not included among Technology Integration monitors or the supported environments listed below) that can forward topology data to BSM using a predefined CI type such as Node, Computer, or some other child CI type derivative. When topology reporting is enabled, SiteScope forwards the topology along with monitor CI data to BSM. For details on this option, see "HP Integration Settings" on page 466. **Note:** This does not include monitors that do not monitor the status of a host or server, since it is not possible to know the CI type that is being monitored in advance. For the list of monitors without host data, see "Monitors Not Reporting Topology Data By Default" on page 302.
Database Environments	(Available when integrating with Business Availability Center version 8.00 and later.) ➤ "DB2 8.x and 9.x Topology" (see *Monitor Reference* in the SiteScope Help) ➤ "Microsoft SQL Server Topology" (see *Monitor Reference* in the SiteScope Help) ➤ "Oracle Database Topology" (see *Monitor Reference* in the SiteScope Help)

Environment/ Monitor Type	Monitors
ERP/CRM Application Environments	(Available when integrating with Business Availability Center/BSM 7.50 and later.) ➤ "SAP CCMS Topology" (see *Monitor Reference* in the SiteScope Help) ➤ "SAP Work Processes Topology" (see *Monitor Reference* in the SiteScope Help) ➤ "Siebel Application Server Topology" (see *Monitor Reference* in the SiteScope Help) ➤ "Siebel Web Server Topology" (see *Monitor Reference* in the SiteScope Help)
SOA Environments	(Available when integrating with Business Availability Center/BSM 7.50 and later.) ➤ "Web Service Topology" (see *Monitor Reference* in the SiteScope Help)
Virtualization Environments	(Available when integrating with Business Availability Center/BSM 8.02 and later.) ➤ "Solaris Zones Topology" (see *Monitor Reference* in the SiteScope Help) ➤ "VMware Performance Topology" (see *Monitor Reference* in the SiteScope Help) ➤ "VMware Host Monitor Topology" (see *Monitor Reference* in the SiteScope Help)
Web server Environments	(Available when integrating with Business Availability Center/BSM 7.50 and later.) ➤ "Microsoft IIS Server Topology" (see *Monitor Reference* in the SiteScope Help) ➤ "WebLogic Application Server Topology" (see *Monitor Reference* in the SiteScope Help) ➤ "WebSphere Application Server Topology" (see *Monitor Reference* in the SiteScope Help)

CI Downtime

Note: This section is relevant only to those users connecting SiteScope with BSM 9.00 or later.

Downtimes are defined and managed in BSM using the Downtime Management page in Platform Admin. For details about configuring downtime, refer to "Downtime Management — Overview" in *Platform Administration* in the HP Business Service Management Documentation Library.

SiteScope is affected by downtime if a SiteScope monitor, measurement, or group CI is directly linked to a CI that BSM detects is in downtime.

Monitors affected by a CI that is currently in downtime do not go into downtime immediately. The time that it takes for the monitors to go into downtime is affected by two configuration parameters:

- The interval between SiteScope queries to BSM for downtime requests (the default downtime retrieval frequency value is 15 minutes). This can be modified in SiteScope in **Preferences** > **Infrastructure Preferences** > **General Settings** > **BSM downtime retrieval frequency (minutes)**.
- The interval between the updates of the SiteScope downtime cache in BSM (the default value is 5 minutes). This can be modified in BSM in **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**:
  - Select **Applications**.
  - Select **End User/System Availability Management**.
  - In the **Downtime** table, locate **SiteScope Downtime Cache Update Interval**. Change the value to the required cache update interval.

The action that is taken in SiteScope during the downtime depends on the downtime configuration in BSM. Downtime can be enforced on the following:

- Alerts. No alerts are sent for any of the CIs associated with the downtime.
- Reports. Reports are not updated and display the downtime for the CI.
- KPIs. KPIs attached to the CI are not updated and display the downtime for the CI in Service Health.
- Monitoring. SiteScope monitoring stops for any of the CIs associated with the downtime.

A monitor that is in downtime is indicated in the SiteScope Dashboard **Summary** column by "disabled by <Downtime Name> from BSM". Details of downtimes that are associated with the monitor and are currently taking place are displayed in the **Monitor Downtime** table in the **Enable/Disable Monitor** pane. For details, see "Enable/Disable Monitor" on page 479.

If the monitor is affected by a CI that is currently in downtime and the downtime applies to associated alerts of the monitor, downtime details are displayed in the **Associated Alerts Downtime** table in the **Enable/Disable Associated Alerts** pane. For details, see "Enable/Disable Associated Alerts" on page 482.

Notes and Limitations

- When SiteScope queries BSM for downtime requests, it gets the downtimes for the downtime period (a maximum of 24 hours). A record is written to the **audit.log** in the **<SiteScope root directory>\logs** directory that includes new downtimes, changes to existing downtimes, and deleted downtimes.
- When SiteScope is connected to BSM 9.00 or later, the downtime mechanism is enabled by default. To change the default setting, clear the **Enable downtime mechanism** check box in **Preferences** > **Infrastructure Preferences** > **General Settings**.
- Downtime is not supported for SAP, Siebel, or SOA topologies (regardless of whether the Application Management for Siebel/SAP license is installed).
- For monitors that report the CI per metric, when a CI connected to a metric is in downtime, this sends the monitor to which the metric belongs into downtime. This is applicable to the "VMware Performance Monitor" and "Solaris Zones Monitor" in the *Monitor Reference*.
- Downtime information is not available in System Availability Management reports.
- For additional troubleshooting relating to CI downtime, see "Business Service Management CI Downtime Issues" in *Best Practices for the SiteScope-Business Service Management/Operations Manager Integration* in the SiteScope Help.

Tasks

How to Configure the Integration Between SiteScope and BSM

This task describes how to configure the integration between SiteScope and BSM.

This task includes the following steps:

1 Prerequisites

- You must be an administrator in SiteScope to integrate SiteScope with BSM. For details on user permissions, see "User Management Preferences Overview" on page 928.
- Prepare a plan that maps out the specific IT infrastructure resources whose data you want to collect. Include information about the business processes that are affected by the specified infrastructure components. For example, business processes being monitored by Business Process Monitor, that are running on an application server against which you plan to run SiteScope monitors.

Note: When connecting SiteScope with BSM 9.x, the **HPOprInf**, **HPOprMss**, **HPOprOra**, and **HPOprJEE** content packs are required (they are installed by default, so you generally do not need to do anything). If you do not have these content packs, you need to import them as described in "How to Create and Manage Content Packs" in *Platform Administration* in the HP BSM Documentation Library.

---

2 Download and install SiteScope

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

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

3 Connect the installed SiteScope with BSM

In BSM, navigate to **Admin** > **System Availability Management**, and add the SiteScope to SAM Administration. For user interface details, see "New SiteScope Page" in *Using System Availability Management* in the HP BSM Documentation Library.

- If you are connecting to a BSM Server different from the one to which SiteScope reports data (for example, where the BSM Gateway Server is installed on a different machine to the Data Processing Server), you must provide connection information for both servers under **Distributed Settings** in SAM Administration's New SiteScope Page (or under the **BSM Integration Main Settings** in SiteScope's Integration Preferences).
- To change logging options, edit a specific monitor and select the relevant option in the **HP Integration Settings** panel of the monitor properties page. For details, see "HP Integration Settings" on page 466. You can use the Global Search and Replace wizard to update the logging options on those monitors created before the integration was established. For details on the wizard, see "Global Search and Replace Wizard" on page 142.
- Monitors created in SiteScope before registration to BSM have their logging option set to **Disable reporting to BSM**. After you configure SiteScope as a data collector reporting to BSM, the default for new monitors created in SiteScope is to log their monitoring data to BSM.

4 Configure SiteScope to connect to a BSM server that requires a client certificate or SSL - optional

If you are using a certificate on the BSM server and want to use that certificate for secure communication with SiteScope, you must perform the appropriate step below:

- For a BSM server that requires SSL, see "How to Connect SiteScope to a BSM Server That Requires SSL" on page 296.
- For a BSM server that requires a client certificate, see "How to Connect SiteScope to a BSM Server That Requires Client Certificate" on page 297.

Note:

- You must specify these settings only if the certificate installed on the BSM 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 BSM server certificate.

---

5 Change the Gateway Server to which SiteScope sends data - optional

You can change the Gateway Server to which a SiteScope reports its data. Generally, this is only applicable if you are working with a BSM deployment with components installed on more than one server.

➤ In SiteScope's BSM Integration Preferences, enter the required Gateway Server name or IP address in the **Business Service Management machine name/IP address** box. For user interface details, see "BSM Integration Preferences Dialog Box" on page 760.

➤ In SAM Admin, update the SiteScope settings with the Gateway Server name in **Distributed Settings**. For user interface details, see "New SiteScope Page" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

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

---

6 Create a monitoring structure in SiteScope

a Create groups and subgroups to organize the monitors to be deployed, and then create monitors in these groups. When configuring monitors, verify that BSM data logging and topology settings are set as required.

For details on creating a monitoring structure, see "How to Configure SiteScope for Monitoring" on page 59.

b Configuring SiteScope to report metrics and to send events to BSM.

For details on configuring BSM metrics integration, see "BSM Integration Data and Topology Settings" on page 467.

For task details on enabling SiteScope to send events to BSM, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326.

7 Create relationships between SiteScope monitors and existing CIs in the RTSM - optional

You can create relationships to enable a monitor to pass HI status information to the CI to which it is attached (even if that CI was not created from a topology forwarded by SiteScope):

- In SiteScope, you can customize the relationship between SiteScope monitor CIs and existing CIs by manually selecting the **CI type** option in **HP Integration Settings** when editing a monitor instance. The CI type is defined by default for monitors of supported environments and monitors that have a defined topology. For task details, see "Select the CI type" on page 299.
- In SAM Admin, by using the **Monitor Deployment Wizard** which uses the existing CI property data in the RTSM to deploy SiteScope monitors, groups, and remote servers. This creates in the RTSM a monitored by relationship between the monitored CI and the created monitor. For concept details, see "Monitor Deployment Wizard Overview" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

Once defined, the SiteScope and its groups and monitors are added as CIs to the RTSM and are automatically attached to the relevant monitor views, from where they can be added to other views. When editing a monitor in SAM Admin, you can associate the monitor with existing CIs using **HP BSM Integration 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 Service Health and Service Level Management.

8 Map SiteScope metrics to indicators - optional

In SiteScope, you can can add mappings for monitors that do not have default indicator metric mappings, or modify settings for existing mappings (monitors of supported environments and monitors that have indicators mapped to metrics by default).

For task details, see "Map Indicators to monitors" on page 300.

9 Assign permissions in BSM

In BSM, navigate to **Admin** > **Platform** > **Users and Permission**, and click **User Management**.

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

For details on how permissions are applied, see "Accessing SiteScope and Building Permissions Model" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

10 Modify the connection settings - optional

After you have created the connection, you can modify the settings either in SiteScope or in BSM, depending on the setting that you are modifying.

➤ In BSM, select **Admin** > **System Availability Management**. In the list of SiteScopes, right-click the relevant SiteScope and select **Edit SiteScope** from the context menu. For user interface details, see "New SiteScope Page" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

➤ In SiteScope, open the **Preferences** context and select **Integration Preferences**. Edit the BSM Integration Preference. For user interface details, see "BSM Integration Preferences Dialog Box" on page 760.

Tip:

➤ To secure the connection to BSM (since the BSM user name and password are not used for authentication), it is recommended to configure either Basic Authentication in SiteScope or use two-way SSL. If BSM is configured to use Basic Authentication, the same user name and password entered in the **Authentication user name** and **Authentication password** fields in SiteScope are used for reporting both data and topology to BSM. If BSM is not configured to use Basic Authentication, the credentials sent are ignored.

➤ To enable data to be compressed before being sent from the SiteScope server to BSM, set **_topazCompressDataInGzip=true** in the **<SiteScope root directory>\groups\master.config** file. When enabled, SiteScope monitor (ss_monitor_t) and SiteScope metric (ss_t) samples are compressed in gzip before being sent to BSM (where it is decompressed). Data compression can be used only when SiteScope is reporting to BAC/BSM 8.05 or later.

How to Connect SiteScope to a BSM Server That Requires SSL

This task describes the steps involved in enabling secure communication between SiteScope and BSM when the BSM server requires SSL.

1. Import the CA or BSM server certificate into SiteScope using Certificate Management in the SiteScope user interface. For task details, see "How to Import Server Certificates Using Certificate Management" on page 910.
2. In BSM, select **Admin** > **System Availability Management Administration**, and click the **New SiteScope** button to add the SiteScope instance. In the New SiteScope page, make sure the following settings are configured:
   - **Distributed Settings:** Check that the **Gateway Server name/IP address** contains the correct server name and port (default 443).
   - **Profile Settings:** Select the **Web Server Use SSL** check box.

How to Connect SiteScope to a BSM Server That Requires Client Certificate

This task describes the steps involved in enabling secure communication between SiteScope and BSM when the BSM server requires a client certificate.

1 Obtain the client certificate in JKS format and copy it to the **SiS\template.certificates** folder.

For details on configuring SiteScope to connect to a BSM server that requires a client certificate, see "Configuring SiteScope to Connect to a BSM Server That Requires a Client Certificate" in the *HP SiteScope Deployment Guide* PDF.

Note: Make sure that the private key password is at least 6 characters long, and that the private key and keystore passwords are the same.

---

2 Edit the **master.config** file in the <**SiteScope root directory**>**groups** using a text editor. Add the following entries with the data indicated:

_urlClientCert=<keystoreName>

_urlClientCertPassword=<keystorePassword>

For example:

```
_urlClientCert=.ks
_urlClientCertPassword=changeit
```

3 Save the changes to the file.

4 Restart the SiteScope server.

How to Configure Topology Reporting

Note: Only advanced users with a thorough knowledge of CIs and indicators should attempt to edit the indicator mappings or to add mappings to metrics.

This task describes how to configure topology settings for monitors. It also describes how to select or modify the CI type and map metrics to indicators.

This task includes the following steps:

- "Prerequisites" on page 298
- "Select the CI type" on page 299
- "Map Indicators to monitors" on page 300
- "Select a preference for influencing BSM Service Health when events and metrics are reported to BSM - optional" on page 300
- "Results" on page 301

1 Prerequisites

- If BSM requires a client certificate, you must configure the topology discovery agent in SiteScope to report topology to the BSM server. For details, see "Configuring the Topology Discovery Agent in SiteScope When BSM Server Requires a Client Certificate" in the *HP SiteScope Deployment Guide* PDF.
- For SiteScope to forward the host topology along with monitor CI data to BSM, the **Report monitor and related CI topology** option must be selected under the **HP Integration Settings** pane in the monitor properties. By default, this option is selected for monitors of supported environments and monitors that have a CI type defined by default.

  For user interface details, see "BSM Integration Data and Topology Settings" on page 467.

2 Select the CI type

For monitors that report a topology by default (the default CI type associated with the monitor is displayed in parenthesis in the **CI type** list), you can use the default selection, or override the selection by modifying the CI type and entering key attributes.

For monitors that do not report a topology by default, select the **CI type** for the monitor in the **BSM Integration Data and Topology Settings** section, and enter values for the CI type key attributes. For the list of monitors that do not report a topology by default, see "Monitors Not Reporting Topology Data By Default" on page 302.

Note: For monitors where the CI type is per metric (for the list of monitors, see "Monitors Reporting CI Per Metric" on page 303), the CI type cannot be modified and CI key attributes are not displayed.

Tip: It is recommended to perform a resynchronization of SiteScope if BSM is restarted within 10 minutes after making changes to a monitor's topology settings. To do so, select **Preferences** > **Integration Preferences** > **BSM Integration** > **BSM Preferences Available Operations**, and click **Re-Synchronize**.

For user interface details, see "BSM Integration Data and Topology Settings" on page 467.

3 Map Indicators to monitors

When a CI type is selected, the table in the **Indicator Settings** section is filtered to show indicator settings for the selected CI type. Monitors of supported environments and monitors that have a defined topology have indicators mapped to metrics by default. You can add new metric mappings or edit settings for existing mappings.

For monitors that do not have default indicator metric mappings, you can map metrics to the appropriate indicators for the CI type linked to the monitor. For the list of default indicator assignments, see "Indicator Mapping Alignment" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

For topic details, see "Assigning SiteScope Metrics to Indicators" on page 279.

For user interface details, see "Indicator Settings" on page 472.

4 Select a preference for influencing BSM Service Health when events and metrics are reported to BSM - optional

Since SiteScope events and metrics can affect BSM's Service Health, select the preference for influencing Service Health when both data types are reported. This preference is relevant only when:

- Both BSM and HP Operations Manager integrations are active.
- The HP Operations Manager event integration is connected to the BSM server—not the HPOM server.
- The following settings are selected in the monitor's HP Integration Settings:
  - In the BSM Integration Data and Topology Settings section: **Enable reporting monitor status and metrics** or **Enable reporting monitor status and metrics with thresholds**.
  - In the HP Operations Manager Integration Settings section: **Send events**.

Select a preference in the **BSM Service Health Preferences** section of **HP Integration Settings**. For user interface details, see "BSM Service Health Preferences" on page 477.

Note:

- The preference can also be set globally for each newly-created monitor in **Integration Preferences** > **HP Operations Manager Integration** > **HP Operations Manager Integration Main Settings**. For user interface details, see "HP Operations Manager Integration Main Settings" on page 777.
- For more information on choosing the preference to use, see "Integrating SiteScope with Business Service Management Applications" in *Best Practices for the SiteScope-Business Service Management/Operations Manager Integration* in the SiteScope Help.

5 Results

After configuring the topology settings click **Save**. SiteScope creates a CI for the monitor in the RTSM and forwards monitor CI data to BSM.

Reference

Monitors Not Reporting Topology Data By Default

Following is a list of those monitors that do not monitor the status of a host or server. For these monitors to report CI information to BSM, you must select the CI type, enter the required CI key attributes, and select an indicator relevant for the CI type linked to the monitor. The monitors include:

- Composite Monitor
- Directory Monitor
- e-Business Transaction Monitor
- File Monitor
- Formula Composite Monitor
- HP NonStop Event Log Monitor
- JMX Monitor (when not monitoring WebLogic)
- Link Check Transaction Monitor
- Log File Monitor
- Microsoft Windows Dial-up Monitor
- Microsoft Windows Media Player Monitor
- Multi Log File Monitor
- Network Bandwidth Monitor
- Real Media Player Monitor
- Script Monitor
- SNMP Trap Monitor

- URL Monitor
- URL Content Monitor
- URL List Monitor
- URL Sequence Monitor
- XML Metrics Monitor

Monitors Reporting CI Per Metric

Following is a list of monitors that report CI per metric. These monitors have multiple CIs; hence the CI and indicator mappings for these monitors cannot be modified.

- SAP CCMS
- SAP Work Processes
- Siebel Application Server
- Siebel Web Server
- Solaris Zones
- VMware Host CPU
- VMware Host Memory
- VMware Host Network
- VMware Host State
- VMware Host Storage
- VMware Performance

Note: You can define a custom topology Node for the monitor and specify a host name for it. If there is a remote server in any SiteScope connected to this BSM, this CI is automatically changed to Unix or Windows CI type, depending on the environment of the remote server.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for BSM integrations.

Tip: We recommend that you only copy these files when the data folder is empty to avoid overloading the system with large amounts of data to upload. When the number of **data.old** folders exceeds a specified threshold, by default 10 folders, the oldest folders are deleted.

Accessing SiteScope from SAM Admin Using Internet Explorer 7

When accessing SiteScope from SAM Admin using Internet Explorer 7, a 408 Request Timeout error is displayed.

Workaround: To be able to log on to SiteScope from BSM, configure the browser to accept cookies from the SiteScope server.

1. In Internet Explorer, select **Tools** > **Internet Options** > **Privacy** tab, and click the **Advanced** button.
2. Select **Override automatic cookie handling**, make sure **First-party cookies** and **Third-party cookies** are set to **Accept**, and select **Always allow session cookies**.

Reporting Data to BSM

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

If SiteScope is unable to connect to the BSM Server, SiteScope continues to record and store monitor data files locally. After the number of data files exceeds a specified threshold, SiteScope saves the data files in a cache folder with the syntax **<SiteScope_root>\cache\persistent\topaz\data<index>.old**. You can configure the number of **data.old** folders to keep by modifying the **_topazMaxOldDirs** property in the **master.config** file.

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.

SiteScope-BSM Integration Troubleshooting

For troubleshooting issues related to SiteScope-BSM metrics integration, CI topology reporting, and CI downtime, see "Troubleshooting SiteScope Integration Issues" in *Best Practices for the SiteScope-Business Service Management/Operations Manager Integration* in the SiteScope Help.

9

Working with Operations Manager and BSM Using the HP Operations Agent

This chapter includes:

Concepts

Tasks

Reference

Concepts

Understanding How SiteScope Communicates with HPOM and BSM

Note: This section is relevant only to those users connecting SiteScope with HP Operations Manager (HPOM) products or to BSM, and only when the SiteScope is reporting to HPOM or BSM version 9.00 or later.

SiteScope, as a standalone application, is an agentless solution for IT infrastructure performance and availability monitoring. SiteScope can also work together with HP Operations Manager (HPOM), HP Performance Manager (a reporting component of HPOM), and Operations Management in BSM, to provide a powerful combination of agentless and agent-based infrastructure management.

SiteScope communicates with these applications using the HP Operations agent, which is installed on the SiteScope server. The HP Operations agent enables SiteScope to integrate both event and metrics data.

- **Events**. The HP Operations agent sends event data to the HPOM management server, or to BSM for use in Operations Management, Service Health, and Service Level Management. Events in SiteScope are based on SiteScope monitor metric status changes and alerts being triggered. For details on enabling event reporting, see "Sending Events" on page 313.
- **Metrics**. The HP Operations agent also acts as a data storage for metrics data collected by SiteScope. This enables SiteScope to make metrics data directly available to Performance Manager (an HPOM reporting component) and to the Performance Perspective tab in BSM's Operations Management. For details on enabling metrics reporting, see "Reporting Metrics Using the HP Operations Agent" on page 322.

Note:

- Metrics integration using the HP Operations agent (where metrics data is used in the Performance Perspective tab in Operations Management) should not be confused with the integration of SiteScope monitor metrics used by the various BSM applications when calculating status for CIs (for example, in Service Health, Service Level Management, and System Availability Management). For details on BSM metrics integration, see "Working with Business Service Management (BSM)" on page 269.
- Metrics integration using the HP Operations agent is supported by SiteScopes running on Windows and UNIX platforms for HPOM and Operations Management.
- SiteScope supports HP Operations agent version 8.60.501.

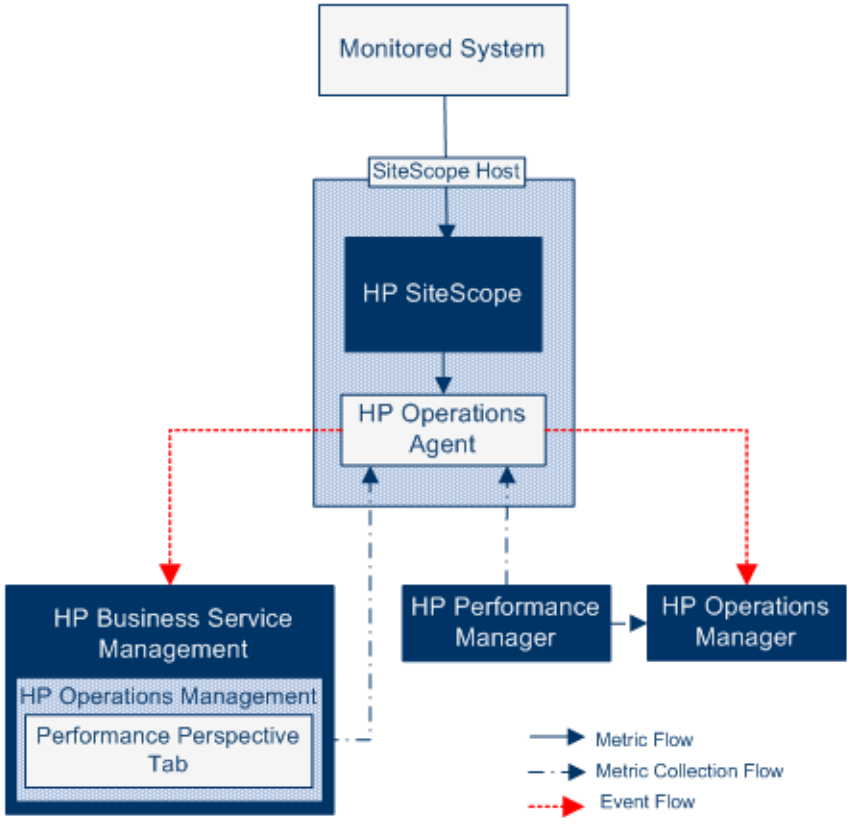
Tip: For best practices and troubleshooting for reporting metrics data to BSM and HPOM products using the HP Operations agent, see Best Practices for the SiteScope-BSM/OM Integration.

The combined functionality of SiteScope and HPOM provides an effective and in-depth monitoring solution. For more details on using HPOM, refer to the HPOM documentation.

This section contains the following topics:

Event and Metrics Flow Diagram

The following diagram illustrates the metrics data and event flow between SiteScope and the HPOM and BSM applications.



HP Operations Agent Topology

HP Operations agent CIs are created when SiteScope is connected to HPOM, and HPOM is connected to BSM.

When SiteScope is connected directly to BSM, SiteScope creates the agent CI through its usual topology flow. When SiteScope sends its main topology (profile CI) and there is either an event or metrics integration with HP Operations Manager active, it also sends the agent topology.

Note:

- The agent CI is deleted only when both event and metrics integrations are removed.
- The agent CI is not deleted when SiteScope is disconnected from BSM since SiteScope does not know if the connection is though HPOM or BSM (the agent CI will eventually disappear due to the aging process).

SiteScope Failover and Operations Manager Integration

If you are using SiteScope Failover to provide backup monitoring availability, the HP Operations agent must be installed on the SiteScope Failover Manager to enable it to send events or store metrics data for integrating with the HPOM management or BSM Gateway Server when the primary SiteScope is down. The agent can be installed during SiteScope Failover installation or after SiteScope Failover is installed using the SiteScope Configuration Tool.

➤ **For Event Integration:** When the primary SiteScope goes down, the SiteScope Failover instance is activated and continues sending events to HPOM/BSM.

Note: The agent on both the failover and primary SiteScope servers must be connected to HPOM, and the SiteScope policies must be uploaded and installed on the agent nodes in HPOM to enable the integration. For configuration details, refer to the *HP SiteScope Failover Manager Guide* PDF.

➤ **For Metrics Integration:** Continuous data graphing can be achieved using the HPOM and BSM reporting tools by selecting both the primary SiteScope and the SiteScope Failover for graphing.

Note: While event integration with HP Operations Manager and BSM and metrics integration with HP Operations Manager can be configured on primary SiteScopes, these integrations are not supported for high availability when Microsoft Cluster Service is used to provide failover monitoring.

For details on using SiteScope Failover, refer to the *HP SiteScope Failover Manager Guide* PDF.

Sending Events

Note: This section is relevant only to those users connecting SiteScope with HP Operations Manager (HPOM) or to BSM, and only when the SiteScope is reporting to HPOM or BSM version 9.00 or later.

You can enable SiteScope to send events directly to the HPOM management server and to BSM (for use in Operations Management, Service Health, and Service Level Management). Events in SiteScope are based on SiteScope monitor metric status changes and alerts being triggered.

To enable SiteScope to send events, the HP Operations agent must be installed on the SiteScope server. The agent can be installed from the SiteScope installation media during SiteScope installation, or after SiteScope is installed using the Configuration Tool. It can also be installed manually from the HPOM management server, although this is not recommended unless it is the same or a later version than the one packaged with SiteScope.

After the agent is installed, it must be configured in SiteScope Integration Preferences. This involves entering the installation path of the agent and the host name or IP address of the HPOM management/BSM Gateway Server, and connecting the agent to HPOM/BSM. The agent then sends a connection request to HPOM/BSM which must grant the certificate request (the HPOM management server can be configured to accept this client automatically).

After the certificate request has been granted on the HPOM/BSM server, a preconfigured log file policy should be installed and signed on the agent installation on the SiteScope server. This enables SiteScope to sign the preconfigured Operations Manager policies locally and automatically. This policy comes with SiteScope, and is deployed from the HP Operations Manager Integration dialog box in SiteScope's Integration Preferences.

When an event is triggered, SiteScope writes the event data to the **HPSiteScopeOperationsManagerIntegration.log** file which is located in the **<SiteScope root directory>\logs** directory. Each event is written as a separate line in the log. The log file policy instructs the agent to read this file and create event messages that are sent to HPOM/BSM.

The format of the event attributes is determined using the event mapping template. The template maps SiteScope runtime data to the event attribute values that are sent to the HPOM management/BSM Gateway Server when an event is triggered. For details on event mappings, see "Common Event Mappings Overview" on page 820.

After the data is converted to an event, the agent sends the event to the HPOM management/BSM Gateway Server. Events are displayed in:

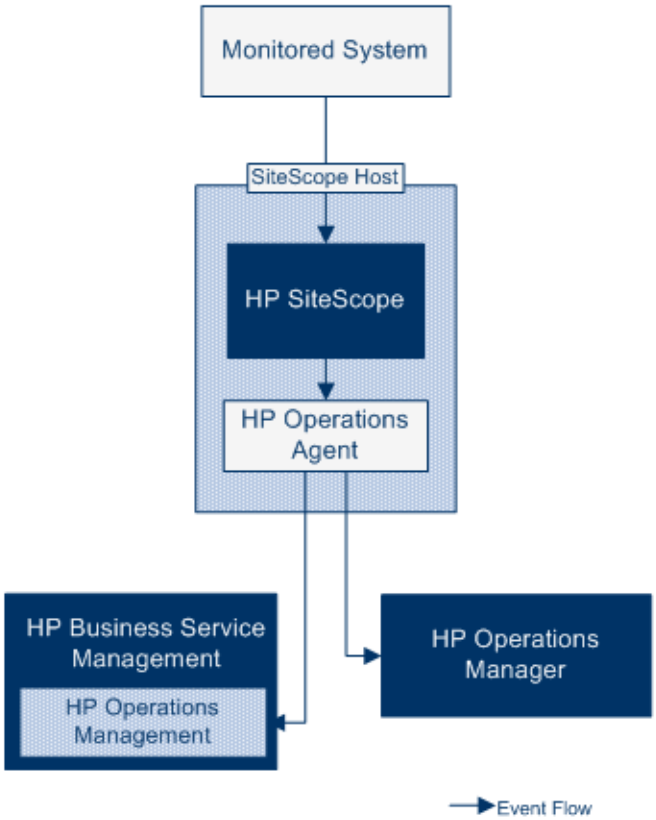
- HPOM's Event Console.
- BSM's Operations Management Event Browser (if you have an Event Management Foundation license) and Service Health (for events that affect CIs). If Operations Management is not part of your BSM installation, you can still view events that affect CI status using a health indicator in Service Health.

For details on configuring SiteScope to send events, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326.

This section also contains the following topics:

Event Integration Diagram

The following diagram illustrates event data flow.



Note: The HP Operations agent can be configured either to report events to an HPOM management or a BSM Gateway Server—not to both.

SiteScope-HP Operations Manager Support Matrix - Event Integration

For the HP Operations Manager versions supported in this release, refer to the HP SiteScope Support Matrices section in the release notes (in SiteScope, select **Help** > **What's New?**).

Event Generation

You can configure events to be generated and sent to the HPOM management server or to Operations Management in BSM following a change in a monitor's metric status or when a SiteScope alert is triggered.

➤ **Status Change**. Every metric or counter status change is an event (for example, if the CPU utilization counter status changes from Good to Error). You can choose whether events are triggered for metrics status changes in the monitor's properties. By default, SiteScope sends an event for each metric status change for the monitor instance.

You can change the default settings for sending events and the event attribute values used when an event is triggered. The event attribute values are filled according to the event configuration mappings using the monitor's properties. For details on event mappings, see "Common Event Mappings Overview" on page 820.

In addition to sending the monitor properties, SiteScope also sends health indicators or event type indicators (indicators) for the monitor instance. Events are categorized according to indicators. The BSM event manager uses indicators to categorize events according to the type of occurrence in the managed IT environment (for example, CPU Load). Indicators that provide CI state information are then used to calculate the CI.

Note: Status change is applicable only to metrics that are configured in the monitor's Thresholds Settings.

➤ **Alert**. Every alert is an event. Since alerts are triggered per monitor, an event triggered by alert can use the monitor's properties, but not the indicators associated with a specific metric. Therefore, when configuring an event alert, you can manually select the indicator that is reported when an event is triggered by an alert. As a result, the indicator is more generic, and you should select indicators that do not affect health indicators in BSM.

Note: In Operations Management, it is recommended to use alert events for notification purposes only.

You can choose whether an alert sends events to HPOM/BSM in the alert definition in the HP Operations Manager Integration Settings pane.

Note:

- When a SiteScope alert is triggered, it is possible that two events are generated if both the alert and monitor are configured to send events. When configuring alerts to send events, you should not also enable the monitors to send events.
- SiteScope also includes threshold information in alerts that are sent to HPOM. In earlier versions of SiteScope and BSM, it was not possible to include the thresholds created for monitors in alerts.

Discovery Scripts and the Drill Down User For Viewing HPOM Events

When SiteScope is integrated with HPOM, the **Node discovery** and **Monitor discovery** policies are activated for nodes and monitors on the HPOM management server. For details, see "Node Discovery Policy" on page 319 and "Monitor Discovery Policy" on page 319.

Both discovery policies rely on the **Integration Viewer** user in SiteScope. This is the user provided by SiteScope for drilling down from HPOM events. This user has been granted view permissions, and permissions to refresh groups and monitors. For details on users and user permissions, see "User Management Preferences" on page 845.

Note:

- The Integration Viewer user is automatically created on SiteScope restart if deleted from User Management Preferences.
- If the Integration Viewer user properties are changed, you must restart SiteScope to update the user properties file, or you can manually update the user properties in the **<SiteScope root directory>\conf\ sitescope_connection.properties** file. When changing Integration Viewer user properties manually, the user login name and password should be encrypted using the SiteScope Encryption Tool. For details on the encryption tool, see "How to Encrypt Text" on page 1068.

For details on deploying the discovery policies on the HPOM management server, refer to the HPOM documentation.

Node Discovery Policy

When SiteScope is connected with HPOM, a node is automatically created and registered in HPOM for each node monitored by SiteScope. This enables SiteScope to report all the nodes that it monitors to HPOM. Only hosts for monitors which report events are sent to HPOM through the discovery policy.

Tip: When you are not connected to HPOM (if connected to Operations Management), it is recommended to disable the node discovery by running the command: ovpolicy -disable -polname SiteScope_Hosts_Discovery

---

Note: SiteScope does not report nodes or services to HPOM for monitors that are disabled, or are not configured to send events.

Monitor Discovery Policy

This is an optional policy that must be activated manually on HPOM using the files in the **<SiteScope root directory>\tools\OMIntegration\SiteScopeMonitorDiscoveryPolicy** directory. After the policy has been activated, SiteScope runs the SiteScope-OM monitor discovery script when it is connected with HPOM.

This policy enables the HPOM Service Navigator to view the SiteScope monitor tree in the HPOM service maps. When new monitors, groups, or both, are added or changes are made in the SiteScope monitor tree, the services tree is updated in HPOM to reflect these changes. In addition, when events arrive to HPOM, they affect the SiteScope services tree and color all related nodes affected by them.

For details on how to enable the monitor discovery policy, see "How to Enable the SiteScope Monitor Discovery Policy" on page 338.

For details on enabling the tool to drill down to SiteScope from HPOM, see "How to Enable the Drill Down to SiteScope Tool on HPOM for Windows" on page 344, and "How to Enable the Drill Down to SiteScope Tool on HPOM for UNIX/Linux/Solaris" on page 346.

Troubleshooting and Limitations

- Upgrades for earlier SiteScope-OM event integration (pre-SiteScope 11.00) are not supported.
- While SiteScope 10.x versions support HPOM event integration, events generated in SiteScope versions earlier than 11.00 do not affect Service Health and Service Level Management in BSM 9.0x.
- Sending events to HPOM using the HP Operations agent is available only when connected to BSM 9.00 or later. Although the earlier HPOM integration solution of installing the HP SiteScope Adaptor on the HPOM management server is supported in earlier versions of SiteScope, it is not supported with SiteScope 11.10 and should be uninstalled. You should therefore upgrade to the new implementation using the HP Operations agent.
- If you are having problems activating node discovery or deploying the monitor discovery policy, verify that the SiteScope node system properties are discovered correctly, and fix them if necessary. In the Node Properties dialog box, select the **System** tab and make sure the settings matches you SiteScope node system settings.
- If you currently use HPOM with SiteScope and you plan to upgrade HPOM to BSM, you must connect SiteScope directly to BSM to perform the upgrade. This also enables SiteScope to report the topology to BSM. For details on connecting SiteScope to BSM, see "Working with Business Service Management (BSM)" on page 269.
- When SiteScope sends an event in which a monitor metric value does not match any of the thresholds, the indicator severity **Normal** is sent to the HPOM management/BSM Gateway Server.

- When SiteScope is connected to BSM, after a monitor is created on a new host, the event is sent to Operations Management without the value of the related CI (the event is triggered before topology is reported to BSM). To avoid waiting for the next event to be sent, select the **Manually send first event** check box in the monitor's **HP Integration Settings** > **HP Operations Manager Integration Settings**. This action can be performed globally using Global Search and Replace.
- Events are not closed (relevant to HPOM and BSM) and the indicator status is not cleared (relevant to BSM) if SiteScope stops monitoring in the following instances:
  - The related SiteScope monitor skipped or was disabled/suspended (permanently or by the scheduler)
  - The related SiteScope monitor was deleted
  - SiteScope stops reporting to BSM (for example, if it is disconnected)
- To exclude indicators of disabled monitors from Service Health, Service Level Management, or both, it is recommended to use Downtime Management in BSM 9.0x. For details, refer to "Downtime Management — Overview" in *Platform Administration* in the HP Business Service Management Documentation Library.
- For additional troubleshooting relating to the HP Operations agent installation, event integration setup, sending events, and with node and monitor discovery, see "Troubleshooting SiteScope Integration Issues" in Best Practices for the SiteScope-BSM/OM Integration in the SiteScope Help.

Reporting Metrics Using the HP Operations Agent

Note: This section is relevant only to those users connecting SiteScope with Operations Management in BSM 9.00 or later, or to HP Performance Manager 9.0 or later, and only when using the HP Operations agent.

SiteScope uses the HP Operations agent to make its metrics data available to HP Performance Manager (the reporting component of HPOM) and to the Performance Perspective tab in BSM's Operations Management. To enable SiteScope metrics to be collected by these reporting products, the HP Operations agent must be installed on the SiteScope server.

Note: Metrics integration using the HP Operations agent (where metrics data is used in the Performance Perspective tab in Operations Management) should not be confused with the integration of SiteScope monitor metrics used by the various BSM applications when calculating status for CIs (for example, in Service Health, Service Level Management, and System Availability Management). For details on BSM metrics integration, see "Working with Business Service Management (BSM)" on page 269.

Metrics integration with Performance Manager can be activated regardless of the connection status between the HP Operations agent and the HPOM/BSM server, since metrics are collected by the agent.

SiteScope collects metrics data, and logs it to the agent data store, which is installed on the SiteScope host. For sizing recommendations, see "Sizing Recommendations for SiteScope-Operations Manager Metrics Integration" on page 356.

When a user in Performance Manager draws or designs a graph, Performance Manager collects metrics data from the agent data store for the selected node in Performance Manager that is monitored by SiteScope, and draws the graph. Agentless graphing is supported in Performance Manager 9.0. For details on Performance Manager, refer to the Performance Manager documentation.

Metrics data collected from SiteScope can also be used in the Performance Perspective tab, the graphing component of BSM's Operations Management.

Metric name alignment, the process of aligning metric names in SiteScope with those used in HPOM/BSM, has been performed for some of the most commonly used monitors. For details, see "SiteScope-Operations Agent Metrics Alignment" on page 352.

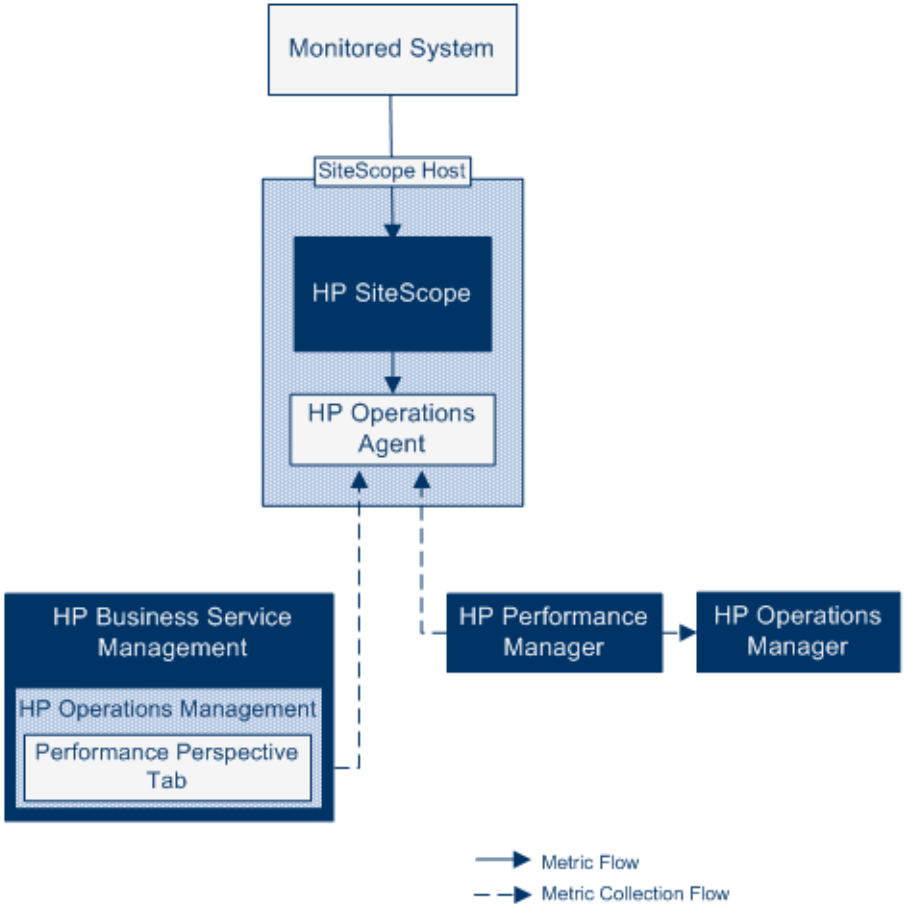
Tip: For best practices and troubleshooting for reporting metrics data to BSM and HPOM products using the HP Operations agent, see Best Practices for the SiteScope-BSM/OM Integration in the SiteScope Help.

For details on configuring metrics integration, see "How to Enable SiteScope to Report Metrics to the HP Operations Agent" on page 349.

This section also contains the following topics:

Metrics Data Flow Diagram

The following diagram illustrates the metrics data flow.



Troubleshooting and Limitations

- The agent data store supports only alphanumeric and the underscore (_) character in SiteScope metric names. All other characters are converted to supported characters (the metric display name (heading) remains in the SiteScope style).
- Web Script monitor data cannot be reported to Operations Management or HPOM.
- After upgrading from HP Performance Manager to BSM's Operations Management (Performance Perspective) and connecting SiteScope to BSM, historical report data cannot be upgraded since it does not have CI-based reporting capability (it can still be viewed in the old HP Performance Manager way).
- To enable reporting numerical values with postfixes (such as 25% or 400MB) to the agent data store, add the list of postfixes, separated by commas, to the **_omMetricIntergationAllowedNumberPostfixs** property in the **master.config** file. For example, to include %, MB, KB, and GB, add **=%,mb,kb,gb**. Note that all postfixes should be in lower case.
- In an Operations Management "manager of managers" configuration (this is where multiple HPOM servers are connected to Operations Management, and multiple SiteScopes are connected to the HPOM servers, and indirectly to Operations Management), data sent from SiteScope is not supported by Performance Perspective in Operations Management, since SiteScope does not send topology to Operations Management. For details on Operations Management deployment configurations, see "Connecting Servers" in *Using Operations Management* in the HP Business Service Management Documentation Library.
- For troubleshooting problems involving HP Operations agent configuration, health monitor errors, and with Performance Manager configuration, see "Troubleshooting SiteScope Integration Issues" in Best Practices for the SiteScope-BSM/OM Integration in the SiteScope Help.

Tasks

How to Enable SiteScope to Send Events to HPOM or BSM

Note: This section is relevant only to those users connecting SiteScope with HP Operations Manager (HPOM) or to BSM, and only when the SiteScope is reporting to HPOM or BSM version 9.00 or later.

This task describes how to enable SiteScope to be used to send events to the HPOM management server or BSM Gateway Server.

This task includes the following steps:

➤ "Configure event mappings for monitors and alerts - optional" on page 335

➤ "Results" on page 335

1 Prerequisites

Only an administrator in SiteScope, or a user granted **Edit integration preferences** and **Edit common event mappings** permissions can create or make changes to Integration Preferences and common event mappings. For details, see "User Management Preferences" on page 845.

2 Install the HP Operations agent on the SiteScope server

You can install the HP Operations agent during SiteScope installation from the SiteScope installation media, or after SiteScope is installed using the Configuration Tool. The agent enables SiteScope to send event data to the HPOM management server or BSM Gateway Server.

For details on installing the agent during SiteScope installation, see "Installing Using the Installation Wizard" in the *HP SiteScope Deployment Guide* PDF.

For details on installing the agent using the Configuration Tool, see "Using the SiteScope Configuration Tool" in the *HP SiteScope Deployment Guide* PDF.

For the list of supported HPOM environments, refer to the HP SiteScope Support Matrices section in the release notes.

3 For BSM on a distributed environment only, configure the connection request to be passed to the Data Processing Server

If BSM uses a separate Gateway and Data Processing Server, perform the following to enable the request received on the Gateway Server to be passed to the Data Processing Server:

a In BSM, select **Admin** > **Platform** > **Infrastructure Settings**:

- ➤ Select **Applications**.
- ➤ Select **Operations Management**.
- ➤ In the **Certificate Server Settings**, locate the **Certificate Server Host**. Make sure that the value matches the host name or IP address of the active BSM Data Processing Server that acts as the certificate server host. If it does not match, change it accordingly.

Note: If the BSM Data Processing Server fails and automatic failover has been configured, you must change the **Certificate Server Host** setting to the name of the backup Data Processing Server to handle new certificate requests. However, if you do not expect any new certificate requests during the Data Processing Server failover timeframe, you can keep the setting unchanged as it does not affect any event integrations configured previously.

---

b On the Gateway Server:

- ➤ Change the active directory to the **\bin** directory by typing cd <HPBSM root directory>\bin.
- ➤ Run **setup-secure-communication.bat** and enter the DNS name of the Data Processing Server.

c On the Data Processing Server:

- Change the active directory to the **\bin** directory by typing cd <HPBSM root directory>\bin.
- Run **setup-secure-communication.bat** and type g to grant the request (make sure that you grant this request and not some other request).

d If you are using a BSM failover environment with load balancer, make sure to keep the certificate server of each Data Processing Server synchronized.

- Repeat steps b and c for every Gateway Server. It does not matter to which Data Processing Server you send the certificate request because the Data Processing Servers already trust each other. As a result, all Gateway Servers trust both Data Processing Servers and can communicate with them regardless of which one is active at any given moment.
- If you install a new certificate on the running Data Processing Server, you also have to install the certificate on the secondary Data Processing Server which is used as failover. To install the new certificate, run the following commands:

  ovcert -importtrusted -file <newCertificateFilePath>

  ovcert -importtrusted -file <newCertificateFilePath> -ovrg server

- Configure the load balancer to forward all HTTPS traffic that arrives on port 383 to the Gateway Servers. This enables the certificate requests and event forwarding to work.

4 Configure the agent connection settings on the SiteScope server

In SiteScope Integration Preferences, configure the HP Operations agent connection settings to the HPOM management server or BSM server.

a Select **Preferences** > **Integration Preferences**, and click **HP Operations Manager Integration** to create a new integration or select an existing integration. For user interface details, see "Integration Preferences Page" on page 757.

b In the HP Operations Manager Integration dialog box, expand the **HP Operations Manager Integration Main Settings** pane, and enter the installation path of the agent and the name or IP address of the HPOM management or BSM server. For user interface details, see "HP Operations Manager Integration Main Settings" on page 777.

c Click **Connect** to connect the agent to the HPOM management or BSM server. This sends a connection request from the agent to the HPOM management or BSM server.

d You can click the **Analyze** button to verify the success of each phase of the process. Use the information supplied in the analysis results to perform problem analysis and for troubleshooting. For example, you can verify connectivity between the agent and server by checking the bbcutil connection protocol.

Note: If an agent is connected to an HPOM or BSM server and you want to connect it to a different server, you must uninstall and reinstall the agent or redirect the agent to another server. For task details, see "How to Reconnect the HP Operations Agent to Another HPOM or BSM Server" on page 336.

---

5 Accept the agent connection request on the HPOM management server or BSM Gateway/Web Processing server

➤ **For HPOM:**

In the HPOM user interface, you need to configure the SiteScope node, map the certificate request to this node, and accept the certificate request. For details, refer to "Configuring Managed Nodes" and "Configuring Certificates" in the "Administering Your Environment" section of the HPOM documentation, or contact your HPOM administrator.

➤ **For BSM:**

For BSM running on a Gateway Server only, perform the following on the BSM Gateway Server. If BSM runs on a distributed environment, perform the following on the Data Processing Server.

a (Optional) To make sure that the OV Certificate Server process is running, run the command line run ovc -status. If it is not running, run the command ovc -start or contact your BSM administrator.

b Change the active directory to the **\bin** directory by typing cd <HPBSM root directory>\bin.

c Run **setup-secure-communication.bat** and type g to grant the request (make sure that you grant this request and not some other request).

d Make sure that the request ID you are going to accept is associated with the agent's core ID. To retrieve the agent's core ID, in SiteScope, click the **Analyze** button in HP Operations Manager Integration, or run the agent's ovcoreid command on the SiteScope server.

6 Install the log policies on the SiteScope server

In the **HP Operations Manager Integrations Main Settings** pane of the HP Operations Manager Integration dialog box, click **Install Policies**. The preconfigured log file policy is installed and signed on the agent.

7 Check connection status and send test message from the SiteScope server - optional

If there are connectivity problems, you can perform problem analysis and check the status of the agent and the certificate request. In the HP Operations Manager Integration dialog box, expand the **HP Operations Manager Integrations Main Settings** pane, and click **Analyze**.

To check that the agent is connected to the HPOM management or BSM server, expand the **HP Operations Manager Integrations Advanced Settings** pane, type a message in the **Test message text** box, and click **Send Test Message**. If the test is successful, the text message is displayed in the HPOM console or in the Operations Management Event Browser inBSM. This message is generated by a basic **opcmsg** policy command.

8 Extend the integration using monitor discovery - optional

To enable the OM Service Navigator to view SiteScope groups and monitors in the OM service maps, you must manually enable the Monitor discovery policy on HPOM using the files in the **<SiteScope root directory>\tools\OMIntegration\SiteScopeMonitorDiscoveryPolicy** directory.

For details on how to enable the policy, see "How to Enable the SiteScope Monitor Discovery Policy" on page 338.

Note: You can also use the Drill Down to SiteScope tool to enable opening the SiteScope user interface from the monitor or group service that was discovered by the monitor discovery policy and added to the HPOM Service Navigator.

- For details on enabling the tool on HPOM for Windows, see "How to Enable the Drill Down to SiteScope Tool on HPOM for Windows" on page 344.
- For details on enabling the tool on HPOM for UNIX/Linux/Solaris, see "How to Enable the Drill Down to SiteScope Tool on HPOM for UNIX/Linux/Solaris" on page 346.

---

9 Enable SiteScope to send events to HPOM or BSM

a In the HP Operations Manager Integration dialog box, expand the **HP Operations Manager Integrations Main Settings** pane, and select **Enable sending events** to enable SiteScope to send events to the HPOM/BSM server.

b To check that the agent can send events to the HPOM/BSM, expand the **HP Operations Manager Integrations Advanced Settings** pane, and click **Send Test Event**. SiteScope writes a test event to the log, which the agent sends to HPOM/BSM.

For user interface details, see "HP Operations Manager Integration Advanced Settings" on page 781.

10 Enable default event severity mappings to be used - optional

In the **Default Severity Mappings** section of the **HP Operations Manager Integrations Advanced Settings** pane, you can enable the default severity mappings that correlate the severity level in HPOM/BSM to the monitor threshold status in SiteScope to be used. These mappings are sent in events triggered by SiteScope alerts, when SiteScope is not connected to BSM, or in any case where the indicator state and severity value is missing (for example, when using monitors that do not have a defined topology). You can also customize the default severity mappings.

For user interface details, see "HP Operations Manager Integration Advanced Settings" on page 781.

Note: You can override the severity mapping at the monitor level by modifying the **Severity** attribute in Common Event Mappings. For details, see step 12 on page 335.

---

11 Enable/Disable sending events for monitor instances and alerts

By default, each newly-created monitor instance is configured to send an event for each metric status change, and each new alert is configured to send an event when triggered. Monitors and alerts that are upgraded from earlier versions of SiteScope are not configured to send events.

- To disable sending events for a monitor instance, in the monitor properties for the selected monitor instance, expand **HP Integration Settings** > **HP Operations Manager Integration Settings**, and clear the **Send events** check box. For user interface details, see "HP Operations Manager Integration Settings" on page 474.
- To disable sending events for an alert, in the New/Edit Alert dialog box, expand the **HP Operations Manager Integration Settings** pane, and clear the **Send events** check box. For user interface details, see "HP Operations Manager Integration Settings" on page 1468.

Note: The **Send events** setting is active only if **Enable sending events** is selected in the HP Operations Manager Integration Main Settings pane of HP Operations Manager Integration Preferences.

---

12 Configure event mappings for monitors and alerts - optional

Monitor instances and alerts are assigned a common event mapping that is used when an event is triggered. This is the mapping between SiteScope runtime data and the values of the attributes of the event that will be sent.

You can use the default event mapping associated with the monitor or alert, select a different event mapping (if any exist), or create a new event mapping in **Preferences** > **Common Event Mappings**. Alternatively, for alerts, you can use the event mapping template associated with the monitor that triggered the alert.

For details of the Common Event Mapping user interface, see "New/Edit Event Mapping Dialog Box" on page 826.

13 Results

After a monitor metric status change or an alert is triggered in SiteScope, the event is written to the integration log file in the format selected for the monitor instance or alert in Common Event Mappings.

The agent monitors the log file and creates an event, which it sends to HPOM or BSM. Events are displayed in the Event Console in HPOM, or in BSM in the Operations Management Event Browser (if you have an Event Management Foundation license). If Operations Management is not part of your BSM installation, you can view events that affect CI status using a health indicator in Service Health.

How to Reconnect the HP Operations Agent to Another HPOM or BSM Server

You can reconnect the HP Operations agent to a different HPOM management or BSM server by uninstalling and reinstalling the agent, or by redirecting the agent to another server.

Note: This task is part of a higher-level task. For details, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326.

To uninstall and reinstall the HP Operations agent:

1. In SiteScope, select **Preferences** > **Integration Preferences**, and delete the HP Operations Manager integration.
2. Open the SiteScope Configuration Tool (**Start** > **Programs** > **HP SiteScope** > **Configuration Tool**), select the **HP Operations Agent** option, and uninstall the HP Operations agent.
3. Open the SiteScope Configuration Tool, select the **HP Operations Agent** option, and install the HP Operations agent.
4. In SiteScope, configure the HP Operations Manager integration with the new HPOM/BSM server to which you want to connect. For user interface details, see "HP Operations Manager Integration Dialog Box" on page 776.

Note: After reconnecting to the HPOM server, it can take some time until events are sent to HPOM. Restarting the HPOM server, the HP Operations agent, or both, might fix it.

To redirect the HP Operations agent to another server:

1. On the SiteScope server where the HP Operations agent is installed, run the following command to create a new core ID: ovcoreid -create -force
2. Run ovcert -list to remove the certificates. For all IDs in the output, run the command ovcert -remove 'id'.
3. Adapt the xpl configuration variable OPC_NODENAME by running the command: ovconfchg -ns eaagt -set OPC_NODENAME 'hostname'
4. Set the new server host name and core ID by running the command:

   ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <new OM server>
   ovconfchg -ns sec.core.auth -set MANAGER <new OM server>
   ovconfchg -ns sec.core.auth -set MANAGER_ID <new OM server ovcoreid>
   ovconfchg -ns eaagt.lic.mgrs -set general_licmgr <new OM server hostname>
   ovconfchg -ns sec.cm.certificates -set CERT_INSTALLED FALSE

5. Restart the HP Operations agent by running the command:

   ovc -kill
   ovc -start

6. Run ovcert -certreq to create a new certificate request.
7. Grant a certificate request on the HPOM/BSM Gateway Server (in case of distributed BSM, grant certificate request on the Data Processing Server).
8. In SiteScope, open the HP Operations Manager Integration dialog box and perform the following in the **HP Operations Manager Integration Main Settings** pane:
   - Change the name or IP address of the HPOM/BSM server in the **HP Operations Manager / BSM host** box. For details, see "HP Operations Manager Integration Main Settings" on page 777.
   - Install the log policies by clicking the **Install Policies** button.

Note: After reconnecting to the HPOM server, it can take some time until events are sent to HPOM. Restarting the HPOM server, the HP Operations agent, or both, might fix it.

How to Enable the SiteScope Monitor Discovery Policy

This task describes how to enhance the SiteScope integration with HPOM by enabling HPOM Service Navigator to view SiteScope groups and monitors in HPOM service maps.

Note:

- This task is part of a higher-level task. For details, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326.
- HPOM 9.0 for Windows 64-bit console does not support the services tree view. The tree view is available in the left pane, but not in the service map on the right.

This task includes the following steps:

1 Copy policy files to the instrumentation folder

On the SiteScope server:

- For Windows: Copy the **discoverSiteScope.bat** file from the **<SiteScope root directory>\integrations\om\bin** folder to the **%OvDataDir%\bin\instrumentation** folder.
- For Linux, UNIX, Solaris: Copy all files from **/opt/HP/SiteScope/integrations/om/bin/*** to the **/var/opt/OV/bin/instrumentation** folder.

Note: All relevant policy files can be found in the **<SiteScope root directory>\tools\OMIntegration\SiteScopeMonitorDiscoveryPolicy\SiS_Discovery_policy_3.0** folder.

---

2 Upload the policy to the HPOM server (for HPOM for Windows servers)

Prerequisites:

- HPOM for Windows 8.16 (or an equivalent patched 8.10 server) or 9.10, and sufficient user rights (typically, Administrator).
- All uploads are performed using the HPOM for Windows command line tool **ovpmutil** which is normally in the environment path.

To upload the policy to the HPOM server:

a Open a command prompt, and navigate to the folder where the SiteScope Discovery 3.0 server components are located. For example, C:\temp\SiS_Discovery_3.0:

```
cd C:\temp\SiS_Discovery_3.0\ForServer
```

b Upload the Service Model using **ovpmutil**:

```
ovpmutil cfg svt upl .\DiscoverSiteScope.mof
```

The Service Model is displayed in the HPOM Service Type Configuration Editor (under **Application Services** > **SiteScope**).

c Upload the SiteScope monitor discovery policy using **ovpmutil** and the provided index file:

```
ovpmutil cfg pol upl .\PolicyConfig_77BFF2F6-38BD-45B3-BEA9-E237C55F7877.xml
```

The policy is now available in the HPOM server policy repository under **Policy management** > **Policy groups**.

3 Upload the policy to the HPOM server (for HPOM for Linux, UNIX, Solaris 9.x servers)

a Upload the HPOM Service Model to the HPOM management server. Open a command shell and type:

```
/opt/OV/bin/OpC/utils/mof_cfgupld.sh /opt/HP/SiteScope/tools/\

OMIntegration/SiteScopeMonitorDiscoveryPolicy/\

SiS_Discovery_policy_3.0/ForServer/DiscoverSiteScope.mof
```

(The .mof file is located in the <**SiteScope**>/**tools**/**OMIntegration**/**SiteScopeMonitorDiscoveryPolicy**/**SiS_Discovery_policy_3.0**/**ForServer** folder.)

b Upload the policies by typing:

```
/opt/OV/bin/OpC/utils/opcpolicy -upload dir=/opt/HP/SiteScope/\

tools/OMIntegration/SiteScopeMonitorDiscoveryPolicy/\

SiS_Discovery_policy_3.0/ForServer
```

c Assign the policies to the node, and deploy to the SiteScope node by typing:

```
# /opt/OV/bin/OpC/utils/opcnode -assign_pol node_name=<NODENAME>
net_type=NETWORK_IP pol_name= "SiteScope Discovery"
pol_type=svcdisc
```

4 Set the Schedule Interval

You can set the schedule interval for running the SiteScope monitor discovery policy on the HPOM agent in the HPOM for Windows console.

a Select **Policy management** > **Policy groups** > **SiteScope Discovery**. In the right pane, right-click **SiteScope Discovery** and select **All Tasks** > **Edit**.

b In the Service Auto-Discovery policy editor, select the **Schedule** tab and specify an interval for running the SiteScope monitor discovery policy on the HPOM agent in the HPOM for Windows console.

5 Deploy the policy

Prerequisites:

- The SiteScope server to be integrated is set up as an HPOM managed node.
- The HP Operations agent is running and connected (for details, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326).
- A certificate has been granted (for details, see "Configuring Managed Nodes" in the "Administering Your Environment" section of the HPOM documentation).
- The SiteScope monitor discovery policy has been uploaded to the **SiteScope Discovery** policy group (for details, see step 2 on page 339 or step 3 on page 340).

To deploy the policy for HPOM for Linux, UNIX, Solaris 9.x servers:

Open a command shell and type: # opcragt -dist <NODENAME>

To deploy the policy for HPOM for Windows servers:

a Right-click the **SiteScope Discovery** policy and select **All Tasks** > **Deploy on**.

b In the Deploy Policies on dialog box, select the SiteScope Server OM node from the available managed nodes, and click **OK**. The deployment status is displayed in **Deployment jobs** in the OM Console.

c To view the policy inventory of the node, right-click the SiteScope Server OM node under **Nodes**, and select **View** > **Policy Inventory**.

d The policy inventory is displayed in the right pane, showing all policies deployed to the node.

6 Manually run the Monitor Discovery policy - optional

For testing or debugging purposes, it is useful to run the discovery manually. This can be done using the **ovagtrep** command line tool on the SiteScope server HPOM agent node where the policy is running.

To do so, run the following commands:

a To force execution of the policy, run the command:

```
ovagtrep -run "SiteScope Discovery"
```

b To force submittal to server, run the command:

```
ovagtrep -publish
```

c For troubleshooting, use the **System.txt** file in the **%OvDataDir%\log** folder.

7 Drill down to the SiteScope user interface from HPOM - optional

You can also use the Drill Down to SiteScope tool to enable opening the SiteScope user interface from the monitor or group service that was discovered by the monitor discovery policy and added to the HPOM Service Navigator.

For details on enabling the tool for HPOM for Windows, see "How to Enable the Drill Down to SiteScope Tool on HPOM for Windows" on page 344.

For details on enabling the tool for HPOM for UNIX/Linux/Solaris, see "How to Enable the Drill Down to SiteScope Tool on HPOM for UNIX/Linux/Solaris" on page 346.

8 Troubleshooting

For troubleshooting, you can check the following files:

- **System.txt** file in the <**SiteScope Server**>**%OvDataDir%\log** folder (for Linux: <**SiteScope Server**>**/var/opt/OV/log**).
- **agtrep.xml** file in <**SiteScope Server**>**%OvDataDir%\datafiles** folder (for Linux: <**SiteScope Server**>**/var/opt/OV/datafile**) to see the discovered instances the agent knows about.
- <**HPOM Server**>**%OvShareDir%\server\log\OvSvcDiscServer.log** to see what the HPOM server receives.

How to Enable the Drill Down to SiteScope Tool on HPOM for Windows

This task describes how to enable the Drill Down to SiteScope tool on the HPOM for Windows management server. This tool enables you to open the SiteScope user interface from the monitor or group service that was discovered by the monitor discovery policy and added to the HPOM Service Navigator.

Note: This task is part of a higher-level task. For details, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326.

This task includes the following steps:

- "Prerequisites" on page 344
- "Install the Drill Down to SiteScope tool on the HPOM for Windows server" on page 345
- "Associate the tool with the SiteScope Service" on page 345
- "Launch the tool (from the SiteScope service)" on page 345
- "Launch the tool (from the Tools repository)" on page 346

1 Prerequisites

The Monitor Discovery policy must be enabled and deployed on the SiteScope Server node on HPOM.

For task details, see "How to Enable the SiteScope Monitor Discovery Policy" on page 338.

2 Install the Drill Down to SiteScope tool on the HPOM for Windows server

a Log on to the HPOM for Windows server machine as an Administrator.

b Copy the **drillDownToSiteScope.vbs** file from the **<SiteScope root>\tools\OMIntegration\DrillDownTool\ForOMW** folder to \\<**HPOM server**>**SPI-Share\SiteScope**.

c Upload the Drill Down to SiteScope tool to the HPOM server:

- Copy the **tls_drillDownToSIS.mof** file from the **<SiteScope root>\tools\OMIntegration\DrillDownTool\ForOMW** folder to any folder on the HPOM server machine (<tls path>).
- Open a command line and run:

```
>> ovpmutil cfg tls upl <tls path>\tls_drillDownToSIS.mof
```

d The Drill Down to SiteScope tool is available on the HPOM server under **Tools** > **SiteScope Tools**.

3 Associate the tool with the SiteScope Service

a In the HPOM for Windows console, open the Service Type Configuration Editor, select **Application Services** > **SiteScope**, and click the **Properties** button.

a In the SiteScope Properties dialog box, click the **Tools** tab, select **SiteScope Tools**, and then click **OK.**

4 Launch the tool (from the SiteScope service)

a In the HPOM for Windows console, right-click the SiteScope service that you want to view (SiteScope monitor, group, or server service), and select **All Tasks** > **Launch Tool**.

b Select the **Drill Down to SiteScope** tool, and click **Launch**.

c The SiteScope user interface opens displaying the selected monitor, group, or the default Dashboard view (if SiteScope Server service was selected).

5 Launch the tool (from the Tools repository)

a In the HPOM for Windows console, expand **Tools** > **SiteScope Tools**. In the right pane, right-click the **Drill Down to SiteScope** tool and select **All Tasks** > **Launch Tool**.

b In the Edit Parameters dialog box, select the monitor, group, or SiteScope Server service that you want to view, and click **Launch**.

c The SiteScope user interface opens displaying the selected monitor, group, or default Dashboard view (if SiteScope Server service was selected).

How to Enable the Drill Down to SiteScope Tool on HPOM for UNIX/Linux/Solaris

This task describes how to enable the Drill Down to SiteScope tools on the HPOM for UNIX/Linux/Solaris management server. This tool enables you to open the SiteScope user interface from events or from the monitor or group service that was discovered by the monitor discovery policy and added to the HPOM Service Navigator.

Note: This task is part of a higher-level task. For details, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326.

This task includes the following steps:

1 Prerequisites

The Monitor Discovery policy must be enabled and deployed on the SiteScope Server node on HPOM. For task details, see "How to Enable the SiteScope Monitor Discovery Policy" on page 338.

2 Install the Drill Down to SiteScope tools on the HPOM for UNIX/Linux/Solaris server

a Log on to the HPOM for UNIX/Linux/Solaris server machine as an Administrator.

b Open a command shell and create a new directory by typing:

```
# mkdir -p /opt/OV/newconfig/SiteScope
```

c Change to the SiteScope directory by typing:

```
cd /opt/OV/newconfig/SiteScope
```

d Copy the **DrillDownToSIS.tar** file from the **<SiteScope root>\tools\OMIntegration\DrillDownTool\ForOMX** folder to **/opt/OV/newconfig/SiteScope** on the HPOM server machine.

e Extract the .tar file to the current directory by typing:

```
# cd /opt/OV/newconfig/SiteScope
# tar -xvf DrillDownToSIS.tar
```

f Upload the Drill Down to SiteScope tools to the HPOM server by typing:

```
# cd /opt/OV/bin/OpC/
# opccfgupld -replace -subentity /opt/OV/newconfig/SiteScope/
DrillDownToSIS
```

g The Drill Down to SiteScope tools are available on the HPOM Administrator user interface under **Browse** > **All Tool Groups**.

h Assign **Drill Down to SiteScope tools** to the **opc_adm** user.

➤ Click **Action** > **Assign to User/Profile...**

➤ Select **All Users** > **opc_adm** and click **OK**.

i Update the HPOM user interface by selecting **File** > **Reload Configuration**.

j The Drill Down to SiteScope tools are available on the HPOM server under **Tools** > **Drill Down to SiteScope tools**.

3 Launch the tool (from the SiteScope service)

a In the HPOM Administrator user interface, right-click the SiteScope service (server, group, or monitor), select **Start** > **Tools** > **Drill Down to SiteScope tools** > **Drill Down to SiteScope service**, and select the tool according to the service type selected.

b The SiteScope user interface opens displaying the selected monitor, group, or default SiteScope Dashboard view.

4 Launch the tool (from an event)

a In the HPOM Administrator user interface, right-click an event and select **Start** > **Drill Down to SiteScope tools** > **Drill Down to SiteScope event**.

b The SiteScope user interface opens displaying the selected monitor that send the event.

How to Enable SiteScope to Report Metrics to the HP Operations Agent

---

Note: This section is relevant only to those users connecting SiteScope with Operations Management in BSM 9.00 or later, or to HP Performance Manager 9.0 or later, and only when using the HP Operations agent.

This task describes how to enable SiteScope to report metrics data to HPOM and BSM reporting products.

This task includes the following steps:

1 Prerequisites

- Only an administrator in SiteScope or a user granted **Edit integration preferences** permissions has the permissions to perform this task. For details, see "User Management Preferences" on page 845.
- Performance Manager administrator must configure Performance Manager to connect to the SiteScope node where the SiteScope instance is logging data. For details, refer to the Performance Manager documentation.

2 Install the HP Operations agent on the SiteScope server

You can install the HP Operations agent during or after a SiteScope installation from the SiteScope installation media. The agent enables SiteScope to act as data storage for metrics data collected by SiteScope.

For details on installing the agent, see "Installing Using the Installation Wizard" in the *HP SiteScope Deployment Guide* PDF.

3 Enable SiteScope to send metrics

In **Preferences** > **Integration Preferences**, select an existing Operations Manager integration or click **HP Operations Manager integration** to create a new integration. In the HP Operations Manager Integration dialog box, expand the **HP Operations Manager Metrics Integration** pane and select **Enable HP Operations Manager metrics integration**.

Note: Metrics integration with HP Operations Manager can be activated regardless of the connection status between the HP Operations agent and the HPOM/BSM server, since metrics are collected by the agent.

For user interface details, see "HP Operations Manager Metrics Integration" on page 782.

4 Enable monitor instances to send metrics

For each monitor instance that you want to report metrics data to the agent data storage, expand **HP Integration Settings** in the monitor properties, and select **Report metrics to HP Operations agent** in the **HP Operations Manager Integration Settings** section.

For user interface details, see "HP Operations Manager Integration Settings" on page 474.

Tip: You can enable reporting metrics for all Memory, CPU, Disk Space, and Windows Resources without having to select **Report metrics to HP Operations agent** in the monitor properties for each monitor instance. To do so, click the **Enable metrics reporting for specific monitors** button in **Integration Preferences** > **HP Operations Manager Integration** > **HP Operations Manager Metrics Integration** pane.

---

5 Results

Each monitor metric is logged as an instance by the agent on the SiteScope host node, with the time and host as the instance identifier. The metrics data is collected from the agent data storage by HPOM and BSM for use in the reporting products.

Metrics error data is written to the **oa_metric_integration.log** file which is found in the **<SiteScope root directory>\logs** directory. For details on using log files, see "Log Files Page" on page 1409.

Reference

SiteScope-Operations Agent Metrics Alignment

Metrics name alignment is the process of aligning metrics names in SiteScope with those used by Operations Manager Performance Agent (PA). Metrics name alignment has been performed for the commonly used metrics listed below.

Note: For more information on metrics provided by Performance Agent, refer to the HP Performance Agent Metric Help Viewer in the Performance Agent 5.0 documentation (http://support.openview.hp.com/selfsolve/document/KM864772/binary/PA5_MetricHelpView.html?searchIdentifier=-65c7a852:127e60d1b54:6921&resultType=document). To enter the HP Software Self-solve knowledge base, you must log on with your HP Passport ID.

PA Metrics Name (Display Name)	SiteScope Metrics Name
BYCPU_CPU_TOTAL_UTIL (Total CPU%)	**Windows:** ➤ CPU Monitor \utilization (cpu #1, cpu #2, etc) ➤ Microsoft Windows Resources Monitor \Processor\{instance}%\ Processor Time **Linux:** UNIX Resources Monitor \Processor\{instance}\System **HP-UX:** N/A **Solaris:** N/A **AIX:** UNIX Resources Monitor \Processor\{instance}\%sys

PA Metrics Name (Display Name)	SiteScope Metrics Name
BYNETIF_IN_BYTE_RATE (In KB Rate)	**Windows:** Microsoft Windows Resources Monitor \Network Interface\{instance}\Bytes Received\sec **Linux:** UNIX Resources Monitor \Network Interface\ReceiveBytes **HP-UX:** N/A **Solaris:** UNIX Resources Monitor \Network Interface\obytes **AIX:** N/A
BYNETIF_OUT_BYTE_RATE (Out KB Rate)	**Windows:** Microsoft Windows Resources Monitor \Network Interface\{instance}\Bytes Sent\sec **Linux:** UNIX Resources Monitor \Network Interface\TransmitBytes **HP-UX:** N/A **Solaris:** UNIX Resources Monitor \Network Interface\rbytes **AIX:** N/A
BYDSK_PHYS_READ_BYTE_RATE (Phys Read KB Rate)	**Windows:** Microsoft Windows Resources Monitor \Physical Disk\{instance}\% Disk Read Bytes\sec **Linux:** N/A **HP-UX:** N/A **Solaris:** UNIX Resources Monitor \PhysicalDisk\nread **AIX:** N/A
BYDSK_PHYS_WRITE_BYTE_RATE (Phys Write KB Rate)	**Windows:** Microsoft Windows Resources Monitor \Physical Disk\{instance}\% Disk Write Bytes\sec **Linux:** N/A **HP-UX:** N/A **Solaris:** UNIX Resources Monitor \PhysicalDisk\nwritten **AIX:** N/A
BYDSK_REQUEST_QUEUE (Req Queue)	**Windows:** Microsoft Windows Resources Monitor \Physical Disk\{instance}\Avg. Disk Queue Length **Linux:** N/A **HP-UX:** N/A **Solaris:** N/A **AIX:** N/A

PA Metrics Name (Display Name)	SiteScope Metrics Name
BYDSK_UTIL (Disk %)	**Windows:** Microsoft Windows Resources Monitor \Physical Disk\{instance}\% Disk Time **Linux:** N/A **HP-UX:** UNIX Resources Monitor \Block device activity\<device>\ %busy **Solaris:** UNIX Resources Monitor \Block device activity\<device>\ %busy **AIX:** UNIX Resources Monitor\Block device activity\<device>\ %busy
FS_SPACE_UTIL (Space%)	**Windows:** Disk Space Monitor \percent full **Linux:** Disk Space Monitor \percent full **HP-UX:** Disk Space Monitor \percent full **Solaris:** Disk Space Monitor \percent full **AIX:** Disk Space Monitor \percent full
GBL_CPU_TOTAL_UTIL (CPU %)	**Windows:** ➤ CPU Monitor \utilization (avgas) ➤ Microsoft Windows Resources Monitor \Processor_Total\ % Processor Time **Linux:** UNIX Resources Monitor \Processor\Total\System **HP-UX:** N/A **Solaris:** N/A **AIX:** UNIX Resources Monitor\Processor\Total\%sys
GBL_MEM_PAGEOUT_RATE (Pg Out Rate)	**Windows:** Microsoft Windows Resources Monitor \Memory\Pages Output/sec **Linux:** N/A **HP-UX:** N/A **Solaris:** UNIX Resources Monitor \Page-out memory and memory freeing activities\ppgout/s **AIX:** N/A

PA Metrics Name (Display Name)	SiteScope Metrics Name
GBL_MEM_UTIL (Memory %)	**Windows:** Memory Monitor \percent used **Linux:** MemoryMonitor \percent used **HP-UX:** MemoryMonitor \ percent used **Solaris:** MemoryMonitor \percent used **AIX:** N/A
GBL_SWAP_SPACE_UTIL (Swap %)	**Windows:** Microsoft Windows Resources Monitor \Memory\ % Committed Bytes In Use **Linux:** N/A **HP-UX:** N/A **Solaris:** N/A **AIX:** N/A

Sizing Recommendations for SiteScope-Operations Manager Metrics Integration

While the default SiteScope configuration enables running thousands of monitors, sizing is important for planning the maximum number of monitors, metrics, and monitors types that can be stored within the SiteScope-HPOM metrics integration.

The sizing should not exceed:

- Maximum insertion rate of 1000 metrics per minute.
- Total retention storage of 1 GB.
- Total retention period of 5 weeks.

Definitions

The following are definitions of the terms used in the validation calculations below:

- **Monitors**. The number of monitors that report metrics to HPOM Performance Manager.
- **Metrics**. The average number of metrics of the above mentioned monitors that report to HPOM Performance Manager.
- **Frequency**. The average frequency at which the above mentioned monitors feed data into the integration.

Validation

When choosing the specific SiteScope monitors and metrics to store within the SiteScope-HPOM metrics integration, you should validate that the insertion and retention rates do not exceed the recommendations. You can do that using the formulae below:

- **Supported Insertion Rate Validation**:
  (Monitors * Metrics) / Frequency <= 1000 metrics/minute
- **Supported Retention Period Validation**:
  (1000 MB) / ((Monitors * Metrics / Frequency) * 0.07 MB) = configured retention period in days (which should be less than the maximum retention period of 5 weeks)

  where 0.07 MB is the storage size for each metric/minute per day.

Example

If you have 2500 monitors that report data using the HPOM metrics integration, and every monitor has 4 metrics, the frequency of these monitors is every 10 minutes, and the average metric storage size per day is 0.07 MB, you will be able to store your historical data for 14 days.

Validation calculations:

- **Insertion Rate Validation**:
  (2500 monitors * 4 metrics) / 10 minutes = 1000 <= 1000 metrics/minute
- **Retention Period Validation**:
  1000 MB / (((2500 * 4 Metrics) / 10 minutes) * 0.07 MB) = 14.28 days (<= 5 weeks)

10

Working with Network Node Manager i (NNMi)

This chapter includes:

Concepts

Tasks

Reference

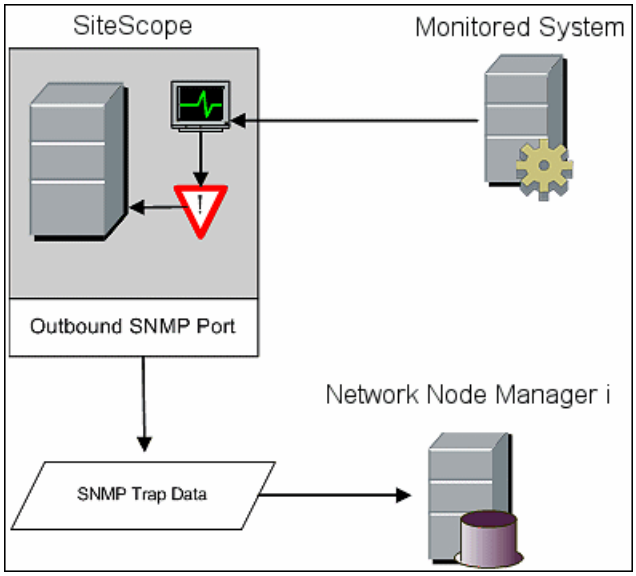
Concepts

Sending SiteScope Events to NNMi

SiteScope can be used as a data collector for Network Node Manager i (NNMi)—an event console used for network monitoring. SiteScope monitors the application side of the system that NNMi is monitoring, and uses SNMP Trap alerts to forward event data from any type of SiteScope monitor to NNMi. Events in SiteScope are based on SiteScope monitor metric status changes and triggered alerts.

SiteScope sends monitor alert SNMP traps to NNMi which are converted to an NNMi incidents. From the resulting incidents, an NNMi console user can launch SiteScope in the context of that monitor (using the URL in the SNMP trap format sent to the NNMi server). For the list of SNMP trap formats used to identify the SiteScope object sending the message to the NNMi server, see "SNMP Trap Format for SiteScope Objects Sent to NNMi" on page 371.

The following diagram illustrates the use of SiteScope as an event data collector for NNMi.



To enable SiteScope to send event data to NNMi, the SiteScope must be configured as a data collector for NNMi. This involves configuring an SNMP preference for the server to which you want to report the SNMP trap, and creating an SNMP Trap alert and assigning it to those monitors that you want to report to NNMi.

For details on configuring SiteScope to send events, see "How to Configure SiteScope to Send Event Data to NNMi" on page 364.

Reporting Metrics to NNMi

SiteScope can also report metrics data to NNMi. To enable SiteScope to report metrics, the Generic Data Integration must be configured on the SiteScope server. The HP NNMi–HP SiteScope System Metrics integration populates the NNM iSPI Performance for Metrics Network Performance Server (NPS) with system metrics data collected by SiteScope monitors. The integration handles data as follows:

1. SiteScope collects monitor data in XML format and passes the collected data to NNMi at the reporting interval of the SiteScope data integration preference.
2. NNMi places the CSV files in the configured location for NPS retrieval.
3. The NPS consumes the CSV files at the NPS accumulation interval.

Supported Versions

The information in this section applies to the following product versions:

- SiteScope version 11.10 or later
- NNMi version 9.10 or later
- NNM iSPI Performance for Metrics version 9.10 or later

For the most recent information about supported hardware platforms and operating systems, see the support matrices for all products.

Supported SiteScope Monitors

While SiteScope reports all monitor types, NNMi only recognizes and forwards data to NPS for consumption from the following SiteScope monitor types:

- CPU Utilization Monitor
- Disk Space Monitor
- Memory Monitor
- Microsoft Windows Resources Monitor
- UNIX Resources Monitor

The nodes being monitored must be managed in NNMi. The integration discards data for nodes that are not in the NNMi topology and for unmanaged nodes.

For details on how to configure SiteScope to communicate with NNM, see "How to Configure SiteScope to Report Metrics Data to NNMi" on page 367.

Note: For details on how configure NNMi to communicate with SiteScope, refer to the *NNMi Deployment Reference* included on the NNMi product media.

Tasks

How to Configure SiteScope to Send Event Data to NNMi

This task describes how to configure SiteScope to send event data to NNMi.

This task includes the following steps:

- "Create an SNMP preference for reporting the SNMP Trap to the NNMi server" on page 364
- "Create an SNMP Trap alert" on page 365
- "Results" on page 366

1 Create an SNMP preference for reporting the SNMP Trap to the NNMi server

In SiteScope, select **Preferences** > **SNMP Preferences**, and create a preference for the server to which you want to report the SNMP trap using the following settings:

- **SNMP trap ID.** Select **Enterprise-Specific SNMP trap ID**, and enter **1**.
- **SNMP object ID.** Select **Preconfigured SNMP object IDs** and choose **HP SiteScope Event** from the list.

Complete the other SNMP trap fields as required.

For user interface details, see "New/Edit SNMP Trap Dialog Box" on page 815.

2 Create an SNMP Trap alert

Create an SNMP Trap alert with SNMP Trap alert action for each status level (Error, Warning, Good, Unavailable).

a In the SiteScope monitor tree, right-click the **SiteScope** root and select **New** > **Alert**.

b In the Alert Targets pane, select the groups, monitors, or both, to trigger this alert. For user interface details, see "New/Edit Alert Dialog Box" on page 1463.

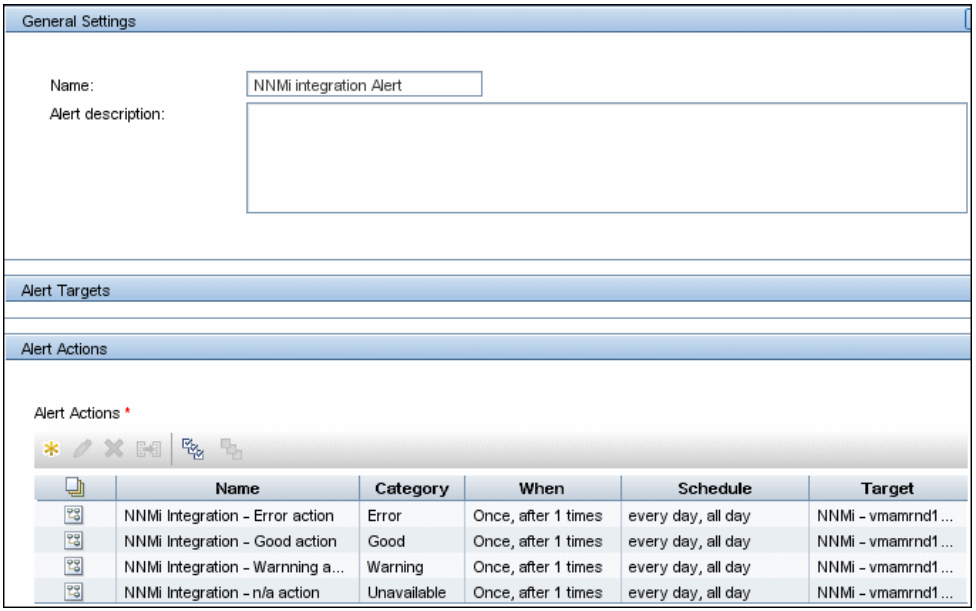
c Create an SNMP Trap alert action for each status level (Error, Warning, Good, and Unavailable).

- In the Alert Actions pane, select **SNMP Trap** action type, and configure an SNMP Trap alert. For user interface details, see "SNMP Trap Alert Properties" on page 1489.
- In the Action Type Settings pane, select **SiteScopeEvent.xml** from the **Template** list. This template contains the format and content of messages sent by SNMP to NNMi when a SNMP trap is triggered. You can copy and customize this template which is located in the **<SiteScope root directory>\templates.snmp**.
- In the Status Trigger pane, select an SNMP trap status. For user interface details, see "Status Trigger Pane" on page 1491.

d Repeat the previous step (create an SNMP trap alert action) for each status in the Status Trigger pane.

Example:

The example shows an NNMi alert with an SNMP trap alert action for each trigger status (Error, Warning, Good, and Unavailable).



3 Results

When a monitor status changes or an alert is triggered in SiteScope, the SiteScope alert reports an SNMP trap to the NNMi server. NNMi reads the SNMP trap, translates the attributes, and displays the SiteScope event data in the NNMi Incidents Console.

For details on the NNMi Incidents Console, refer to *NNMi Deployment Reference* included on the NNMi product media.

How to Configure SiteScope to Report Metrics Data to NNMi

This task describes how to configure SiteScope to report metrics data to NNMi.

This task includes the following steps:

- "Enable the integration on the NNMi server" on page 367
- "Configure SiteScope to communicate with NNMi using SSL" on page 367
- "Create a search/filter tag to identify the NNMi server" on page 368
- "Configure the connection between SiteScope and the NNMi server" on page 368
- "Configure the monitors that contribute to SiteScope reports on the NNMi server" on page 369
- "Results" on page 370

1 Enable the integration on the NNMi server

For details on how configure the NNMi metrics integration in the NNMi console, see "HP NNMi—HP SiteScope System Metrics Integration" in *NNMi Deployment Reference* included on the NNMi product media.

2 Configure SiteScope to communicate with NNMi using SSL

a In SiteScope, select **Preferences** > **Certificate Management**, and click the **Import Certificates** button. Select **File** or **Host**, and enter the details of the source server. For user interface details, see "Import Certificates Dialog Box" on page 914.

b Under **Source Selection**, provide information to identify the NNMi management server to SiteScope:

- Select **Host**, and enter the fully-qualified domain name of the NNMi management server.
- If necessary, change the port number to match the HTTPS port on the NNMi management server.

c Click **Load**. The NNMi certificate information appears under **Loaded Certificates**. Note the certificate alias.

d Select the NNMi certificate, and then click **Import**. The imported certificate is listed on the Certificate Management keystore list.

3 Create a search/filter tag to identify the NNMi server

a In SiteScope, select **Preferences** > **Search/Filter Tags**, and click the **New Tag** button. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

b Enter a tag name (for example, NNMi_upload) and at least one value.

4 Configure the connection between SiteScope and the NNMi server

a In SiteScope, select **Preferences** > **Integration Preferences**. Click the **New Integration** button, and then click **Data Integration**. For user interface details, see "Data Integration Preferences Dialog Box" on page 766.

b Under **General Settings**, enter a name (for example, NNMi_receiver) and a description (optional).

c Under **Data Integration Preferences Settings**, include the following settings:

- In the **Receiver URL** field, paste the URL returned after enabling the integration in the NNMi Console (for example: https://nnmi_server.example.com:443/sitescope-adapter/sitescopereceiver).
- Select the **GZIP compression** check box.
- Clear the **Include additional data** and **Error on redirect** check boxes. (These are the default settings.)
- Select the **Authentication when requested** check box. (This is the default setting.)
- Clear the **Disable integration** check box. (This is the default setting.)
- For all other settings, the default configuration is acceptable.

d Under **Web Server Security Settings**, enter the user name and password for the NNMi user that was specified on the integration configuration form in the NNMi console. Contact your NNMi administrator for assistance.

e Under **Reporting Tags**, select the search/filter tag that you created in the step 3 (for example, NNMi_upload).

5 Configure the monitors that contribute to SiteScope reports on the NNMi server

a Create new monitors or identify existing monitors of the supported types (as required):

- CPU Utilization Monitor
- Disk Space Monitor
- Memory Monitor
- Microsoft Windows Resources Monitor
- UNIX Resources Monitor

Configure monitor settings. For a description of the monitor settings, see the help for the specific monitor in *Monitor Reference*.

For the list of available counters, see "SiteScope Monitor Metrics Reported to NNMi" on page 374.

b Add the search/filter tag that you created in step 3 (for example, NNMi_upload) to the monitors that should pass data to NNMi.

The integration can only process data for managed nodes in the NNMi topology. So, only apply the tag to monitors on nodes in the NNMi topology.

Tip: It is recommended to organize the monitors that pass data to NNMi into one monitor group.

---

6 Results

The NNM iSPI Performance for Metrics Network Performance Server (NPS) is populated with system metrics data collected by SiteScope monitors.

For more details, refer to *NNMi Deployment Reference* included on the NNMi product media.

Reference

SNMP Trap Format for SiteScope Objects Sent to NNMi

Following is a list of SNMP trap formats used to identify the SiteScope object sending the message to the NNMi server. This enables an NNMi console user to launch SiteScope in the context of that monitor.

The SNMP trap formats are stored in the **SiteScopeEvent.xml** file which is located in the **<SiteScope root directory>\templates.snmp** folder.

Field Name	Object ID (OID)	Description	Values
Enterprise OID	.1.3.6.1.4.1.11.15.1	SiteScope root Object ID	.1.3.6.1.4.1.11.15.1
Trap OID	.1.3.6.1.4.1.11.15.1.0	SNMP Trap Object ID	(OID) For V1: [1.3.6.1.4.1.11.15.1.4.0.1] For V2: [1.3.6.1.4.1.11.15.1.4.1]
SiteScope Host	.1.3.6.1.4.1.11.15.1.1.2	IP address or host name of the SiteScope server	(IpAddress) [16.55.244.182] or (OctetString) [sisserver.mydomain]
Provider (Collector)	.1.3.6.1.4.1.11.15.1.1.3	SiteScope application name	(OctetString) SiteScope
Monitor Name	.1.3.6.1.4.1.11.15.1.2.1.1	SiteScope monitor name	(OctetString) [Memory monitor on myhost.mydomain]
Monitor Type	.1.3.6.1.4.1.11.15.1.2.1.2	SiteScope monitor type	(OctetString) [Memory Monitor]

Field Name	Object ID (OID)	Description	Values
Monitor ID	.1.3.6.1.4.1.11.15.1.2.1.3	Monitor unique ID	(OctetString) [067e6162-3b6f-4ae2-a171-2470b63dff00]
Monitor Drill Down URL Secured	.1.3.6.1.4.1.11.15.1.2.1.4	URL that opens SiteScope in context of the alerted monitor, without silent login information. This allows configuration per integration instance level. To get drill down URL with user credentials, change the reference value from **monitorDrilldownUrl Secured** to **monitorDrilldownUrl**.	(OctetString) [http://sisserver:8080/SiteScope/servlet/Main?activeid=__SiteScope Root__&activerighttop=dashboard&view=new&dashboard_view=Details&dashboard_model=true&dashb
Monitor Target Host	.1.3.6.1.4.1.11.15.1.2.1.5	Monitor target host	(IpAddress) [16.55.244.182] or (OctetString) [myhost.mydomain]
Monitor Target IP	.1.3.6.1.4.1.11.15.1.2.1.6	Monitor target IP address	(IpAddress) [16.55.244.182]
Monitor Full Name	.1.3.6.1.4.1.11.15.1.2.1.7	SiteScope monitor name including full path from the root.	(OctetString) [Memory monitor on myhost.mydomain]
Title	.1.3.6.1.4.1.11.15.1.3.1.1	SiteScope Event Title	(OctetString) [Alert 'Memory Alert' was triggered on monitor 'Memory monitor on myhost.mydomain' due to a status change]

Field Name	Object ID (OID)	Description	Values
Event Source	.1.3.6.1.4.1.11.15.1.3.1.2	Source of the event (alert or metric)	(OctetString)
Severity	.1.3.6.1.4.1.11.15.1.3.1.3	SiteScope event severity	(Integer) [0,1,2,3] For [unavailable, good, warning, error]
Event Time	.1.3.6.1.4.1.11.15.1.3.1.4	Original event time in milliseconds	(TimeTicks) 1287316779
Value	.1.3.6.1.4.1.11.15.1.3.1.5	(Not for alerts flow)	(OctetString) [running] or [25] or [n/a] - for alerts
Event Description	.1.3.6.1.4.1.11.15.1.3.1.6	Description of fired event	(OctetString)
Event Key	.1.3.6.1.4.1.11.15.1.3.1.7	Key of the event	(OctetString) [sisserver:067e6162-3b6f-4ae2-a171-2470b63dff00:Memory
Event Close Key Pattern	.1.3.6.1.4.1.11.15.1.3.1.8	Key to identify paring events	[sisserver:067e6162-3b6f-4ae2-a171-2470b63dff00]

SiteScope Monitor Metrics Reported to NNMi

Following is a list of SiteScope monitor metrics that are reported to the NNMi server.

Monitor	Available Metrics
CPU Utilization	➤ CPU Utilization **Note:** SiteScope delivers CPU utilization data collected on the HP-UX and AIX operating systems as a single average value for the system, not per specific CPU. Because the integration does not send average values to NNMi, CPU utilization data is not available for the HP-UX and AIX operating systems.
Disk Space	➤ Disk MB Free ➤ Disk Percent Full
Memory	➤ Memory MB Free ➤ Memory Pages/Sec ➤ Memory Percent Used

Monitor	Available Metrics
Microsoft Windows Resources	➤ Windows Process – Percent Privileged Time ➤ Windows Process – Percent Processor Time ➤ Windows Process – Percent User Time ➤ Windows Process – Creating Process ID ➤ Windows Process – Elapsed Time ➤ Windows Process – Handle Count ➤ Windows Process – ID Process ➤ Windows Process – IO Data Bytes/sec ➤ Windows Process – IO Data Operations/sec ➤ Windows Process – IO Data Other Bytes/sec ➤ Windows Process – IO Read Bytes/sec ➤ Windows Process – IO Read Operations/sec ➤ Windows Process – IO Write Bytes/sec ➤ Windows Process – IO Write Operations/sec ➤ Windows Process – Page Faults ➤ Windows Process – Page File Bytes ➤ Windows Process – Page File Bytes Peak ➤ Windows Process – Pool Nonpaged Bytes ➤ Windows Process – Pool Paged Bytes ➤ Windows Process – Priority Base ➤ Windows Process – Private Bytes ➤ Windows Process – Thread Count ➤ Windows Process – Virtual Bytes ➤ Windows Process – Virtual Bytes Peak ➤ Windows Process – Working Set ➤ Windows Process – Private Working Set ➤ Windows Process – Working Set Peak
UNIX Resources	➤ Unix Process – CPU Percent ➤ Unix Process – Memsize ➤ Unix Process – Number_Running ➤ Unix Process – PID

Troubleshooting and Limitations

This section describes troubleshooting and limitations when integrating SiteScope with NNMi.

➤ **Troubleshooting the Event Integration**

If the NNMi incident views do not contain any SiteScope monitor alert incidents, verify in SiteScope that at least one monitor alert has been configured to send SNMP traps to NNMi. For details, see "Create an SNMP Trap alert" on page 365.

For troubleshooting the integration from the NNMi side, refer to the "Troubleshooting the HP NNMi—HP SiteScope Events Integration" section in *NNMi Deployment Reference*.

➤ **Troubleshooting the Metrics Integration Data Flow**

Check the SiteScope error log files (**data_integration.log**) for messages relating to problems with the data integration. For more information, see "Using Log Files" on page 1376.

For troubleshooting the integration from the NNMi side, refer to the "Troubleshooting the HP NNMi—HP SiteScope System Metrics Integration" section in *NNMi Deployment Reference*.

Part IV

Monitors

11

Working with SiteScope Groups

This chapter includes:

Concepts

Tasks

Reference

Concepts

SiteScope Groups Overview

A group is a collection of one or more monitors. It might contain several of one type of monitor, such as URL monitors, or several different monitors that track a specific part of your Web environment, such as a Web server, URL, and network parameters related to a specific transaction. You create group containers to make the deployment of monitors and associated alerts manageable and effective for your environment and organization. It is also useful to group monitors that should generate similar alerts.

Each SiteScope monitor instance that you create must belong to a SiteScope group, either a top level group or a subgroup nested within other group containers.

For example, if you intend to monitor a large number of processes running on your system, you may want all of them to be in a single group named **Processes**. If you are monitoring processes on several machines using remote monitors, you could create a primary group called **Processes** with several subgroups named after each of the remote machines that you are monitoring.

When you add a new monitor you either add it to an existing group, or you must first create a group for it. You can add groups individually to SiteScope, or you can deploy groups along with multiple monitors by using templates. For details on templates, see "SiteScope Templates Overview" on page 944.

You can perform mass operations on group objects using the Manage Groups and Monitors feature. This enables you to perform move, copy, delete, run monitors in group, enable/disable monitors, and enable/disable associated alert actions on multiple SiteScope objects. For details, see "Manage Monitors and Groups Dialog Box" on page 77.

Note: You can also use the SiteScope API when working with groups. For details, see "Using the SiteScope Configuration API" on page 42.

This section contains the following topics:

Copying or Moving Existing Groups

In addition to creating groups, you can copy or move existing groups to a new location within the SiteScope tree. Copying or moving a group duplicates the configuration settings for the group and all monitors within the group. After copying or moving a group, you normally need to edit the group and the configuration properties for each individual monitor within the group to direct the monitors to a unique system or application. Otherwise, the monitors in the group duplicate the monitoring actions of the original group.

Tip: Instead of copying groups which can lead to redundant monitoring, use templates to more efficiently replicate common group and monitor configuration patterns. For more information about working with templates, see "SiteScope Templates".

Note:

➤ To avoid group identity problems within SiteScope, object names must be unique within the parent group. If you copy or move a group to another group in which there is group with exactly the same name, SiteScope automatically adds a suffix (number) to the end of the copied/moved group's name.

➤ You cannot move or copy a monitor group to its subgroup.

Creating Group Alerts and Reports

After creating a group, you can create alerts and reports for the group. By default, group alerts and reports are associated with all monitors within the group.

You create an alert by adding an alert definition to a group container. This means that when any one monitor in the group reports the status category defined for the alert (for example, error or warning), the group alert is triggered. You can configure a group alert to exclude one or more of the monitors in the group by using the **Alert targets** selection tree. For details on this topic, see "SiteScope Alerts Overview" on page 1417.

You create a group report by adding a report definition to a group container. You can configure a group report to exclude one or more of the monitors in the group by using the **Monitors and groups to report on** selection tree. For details on this topic, see "SiteScope Reports Overview" on page 1502.

If you delete a group, SiteScope removes the applicable monitor actions and disables any alert actions associated with the group.

Tasks

How to Manage a Group

This task describes the steps involved in managing a group.

This task includes the following steps:

1 Create SiteScope groups and subgroups

Create groups according to the monitor hierarchy which you want to implement. For example, you can create groups of locations, server types, network resources, and so forth.

- **Create a new group.** Right-click the SiteScope or group container in which to create the group, and select **New** > **Group**. For user interface details, see "New SiteScope Group Dialog Box" on page 387.
- **Create a group by copying or moving an existing group.**
  - Right-click the group you want to copy, and click **Copy**. Right-click the location in the monitor tree where you want to copy the group container, and click **Paste**.
  - Right-click the group you want to move, and click **Cut**. Right-click the location in the monitor tree where you want to move the group container, and click **Paste**.
  - To copy or move multiple monitors and groups to a target group, click the **Manage Monitors and Groups** button in the monitor tree toolbar. Select the objects for copying or moving and click **Copy/Cut**. Select the destination group and click **Paste**. For user interface details, see "Manage Monitors and Groups Dialog Box" on page 77.

2 Create monitor instances

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

For task details, see "How to Deploy a Monitor" on page 414.

3 Add URL links to group descriptions - optional

You can add additional information to describe a group, and include HTML tags for hyperlinks to enable you to access URLs from the SiteScope Dashboard.

a To add a hyperlink, open the Properties tab for the selected group.

b Expand the **General Settings** pane and enter the URL in the **Group description** field. For example, My Link.

c Click the **Dashboard** tab. A URL is displayed in the **Description** field for the selected group. To open the URL, click the group's **Description** field, and then click the link.

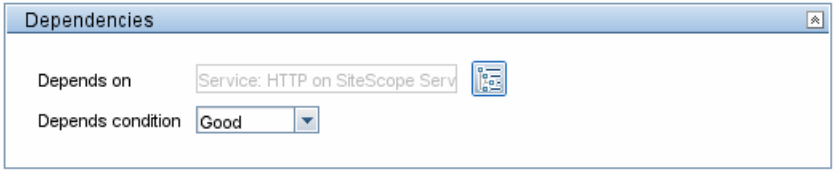
4 Set group dependencies - optional

You can set group dependencies to make the running of monitors in this group dependent on the status of another monitor.

For concept details, see "Monitoring Group Dependencies" on page 397.

Example:

The monitors in the group being configured run normally as long as the monitor selected in the **Depends on** box reports the condition selected in the **Depends condition** box. In this example, the group being configured is enabled only when the **Service** monitor reports a status of **Good**.



5 Set up group alerts - optional

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

To create an alert for the group, right-click the group and select **New > Alert**. For each alert scheme, you can create one or more alert actions. In the New Alert dialog box, click **New Alert Action** to start the Alert Action wizard.

For task details, see "How to Configure an Alert" on page 1443.

6 Set up group reports - optional

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

To create a report for the group, right-click the group and click **Reports**. Select a report type and configure the report settings.

For task details, see "How to Create a Report" on page 1508.

7 Results

The monitor group, including its monitors, alerts, and reports, is added to the monitor tree.

Reference

New SiteScope Group Dialog Box

The New SiteScope Group dialog box enables you to define a new group for SiteScope, or a subgroup for an existing monitor group.

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope container or an existing monitor group, and select **New** > **Group**.
Important information	➤ You cannot delete a monitor group if it has dependent alerts or reports at the container level. To delete a monitor group with dependencies, you must remove the monitor group from **Alert Targets** and **Report Targets** for each dependency, and then delete the monitor group. You can delete monitor groups that have dependencies at the child level. ➤ You can also use the SiteScope API when working with groups. For details, see "Using the SiteScope Configuration API" on page 42.
Relevant tasks	"How to Manage a Group" on page 383
See also	➤ "SiteScope Groups Overview" on page 380 ➤ "Monitor Tree" on page 81

The following elements are found throughout the New SiteScope Group dialog box:

General Settings

UI Element	Description
Group name	Name that describes the content of the group, or the purpose of the monitors added to the group. For example, <host_name> or <business_unitresource_name> or <resource_type>. **Note:** ➤ The group name cannot be **sitescope** or contain any of the following characters: ‘ ; & | < > / \ + = ➤ The group name is case sensitive. This means that you can have more than one group with the same name provided they each have a different case structure.
Group description	Description of the group. This can include the most common HTML tags for text styling, such as , <HR>, and <B>, and hyperlinks. The description is displayed only when viewing or editing the group’s properties in the SiteScope Dashboard. For details on adding a hyperlink, see "Add URL links to group descriptions - optional" on page 385. **Note:** This field does not support JavaScript/iframes/frames or other advanced features. HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. The following is prohibited HTML content: ➤ Tags: **script**, **object**, **param**, **frame**, **iframe**. ➤ Any tag that contains an attribute starting with **on** is declined. For example, onhover. ➤ Any attribute with **javascript** as its value.

UI Element	Description
Source template	Displays the path of the source template if the group was created from a template. If you are using deployed templates created in older versions of SiteScope, enables you to manually associate the root groups with the source template by entering the path of the source template.
Clear	Removes the source template associated with the root group.

Dependencies

UI Element	Description
Depends on	The monitor on which you want to make the running of this monitor group dependent. Click the **Depends on**  button to open the Select Depends On Monitor dialog box, and select the monitor on which you want to create a dependency. For user interface details, see "Select Depends On Monitor Dialog Box" on page 487. For concept details, see "Monitoring Group Dependencies" on page 397. **Default**: No dependency is set for a monitor group.
Depends condition	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** box is automatically disabled. The conditions are: ➤ Good ➤ Error ➤ Available

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

12

Working with SiteScope Monitors

This chapter includes:

Concepts

Tasks

Reference

Concepts

SiteScope Monitors Overview

SiteScope monitors are tools for automatically connecting to and querying different kinds of systems and applications used in enterprise business systems. The different monitor types provide the generic capabilities for performing actions specific to different systems. You create one or more instances of a monitor type to instruct SiteScope how to monitor specific elements in your IT infrastructure.

For example, you can create 100 monitor instances that instruct the SiteScope CPU Monitor type to connect to and measure CPU utilization on remote servers. Each monitor instance contains a different setting defining which remote server is to be monitored and how often. SiteScope is then configured to automatically monitor the CPU utilization on 100 servers at regular intervals.

Monitor instances that you create must be added within a SiteScope monitor group container. You use group containers to help you organize the monitor instances that you create.

Note:

- For details on the monitor settings for a specific SiteScope monitor, see the monitor type in the *Monitor Reference* guide.
- For a list of counters or metrics that can be configured for SiteScope monitors, as well as versions of applications or operating systems that are supported, see the HP SiteScope Monitors and Metrics document located in **<SiteScope>\sisdocs\pdfs\SiteScope_Monitors_Metrics.doc**.
- You can also use the SiteScope API when working with monitors. For details, see "Using the SiteScope Configuration API" on page 42.

SiteScope Monitor Categories

SiteScope monitor categories are grouped according to classes that indicates their availability and category that reflect their function. When you select to add a new monitor to a SiteScope agent, the list of available monitor types for that agent are displayed both alphabetically and divided by category in the product interface. The availability of the monitor category is dependent on the class of monitor. This section describes the monitor classes and the category listing formats.

This section contains the following topics:

Standard Monitors

Standard monitor categories represent the monitor categories available with a general SiteScope license. These monitor categories include many of the general purpose monitor categories.

- **Application Monitors**. Monitors in this category monitor third party applications. These monitors enable SiteScope to access and retrieve data from the monitored applications.
- **Database Monitors.** Monitors in this category monitor different types of database applications. There are monitors that access data from specific database applications and generic monitors that can be configured to monitor any database application.
- **Generic Monitors.** Monitors in this category monitor different types of environment. These monitors can monitor networks, applications, and databases depending on how they are configured.
- **Network Monitors.** Monitors in this category monitor network health and availability.
- **Server Monitors.** Monitors in this category monitor server health and availability.

- **Media Monitors.** Monitors in this category monitor applications that play media files and stream data.
- **Web Transaction Monitors.** Monitors in this category monitor web-based applications.
- **Virtualization Monitors.** Monitors in this category monitor virtualization technologies.
- **Virtualization and Cloud Monitors.** Monitors in this category monitor virtualized environments and cloud infrastructures.

To see the list of monitors contained in each monitor category, see "Monitor Categories List" on page 428.

For information about the usage and configuring each monitor type, see the monitor type in the *Monitor Reference* guide.

Integration Monitors

This group of optional monitor types are used to integrate HP products with other commonly used Enterprise Management systems and applications.

These monitor types require additional licensing and may only be available as part of another HP product. For more information about Integration Monitor capabilities, see the section on "Working with SiteScope Integration Monitors" on page 521.

To see the list of monitors contained in each monitor category, see "Monitor Categories List" on page 428.

For information about the usage and configuring each monitor type, see the monitor type in the *Monitor Reference* guide.

Solution Template Monitors

Solution template monitor types are a special class of monitors that enable new monitoring capabilities for specific applications and environments. As part of a solution template, these monitor types are deployed automatically together with other, standard monitor types to provide a monitoring solution that incorporates best practice configurations. These monitor types are controlled by option licensing and can only be added by deploying the applicable solution template. After they have been deployed, you can edit or delete them using the same steps as with other monitor types. For more information, see "SiteScope Solution Templates" on page 1083.

The monitor types using solution templates include:

- Active Directory (with and without Global Catalog)
- HP Service Manager
- Microsoft Exchange
- Microsoft IIS Server
- Microsoft Lync Server
- Microsoft SQL Server
- Microsoft Windows Resources
- Oracle Database
- SAP Application Server
- Siebel Application/Gateway/Web Server (for UNIX and Windows)
- UNIX Resources
- VMware Host CPU/Memory/Network/State/Storage
- WebLogic Application Server
- WebSphere Application Server

Monitoring Remote Servers

Some SiteScope monitors use Internet protocols to test Web systems and applications. Other SiteScope monitors use network file system services and commands to monitor information on remote servers.

Monitoring remote Windows servers requires:

- SiteScope for Windows XP/2000/2003/2008. In general, SiteScope for UNIX cannot monitor remote Windows servers.
- The SiteScope service must run in a user or administrative account that has permission to access the Windows Performance registry on the remote servers to be monitored. For details on how to change the SiteScope account user, see "Change the User Account of the SiteScope Service" on page 592.

To monitor certain server level parameters on a remote server using the network files system services, you must create a remote server profile. A table of server profiles is listed on the Microsoft Windows/UNIX Remote Server page in the remote server view. The remote server profiles contain the address and connection information that SiteScope needs to make a remote connection. After creating remote server profiles, set up monitors to use the remote connection profile. For details on creating remote profiles and remotely monitoring either Windows or UNIX servers, see "Remote Servers Overview" on page 584.

The requirements for monitoring services and applications that are running on remote servers vary according to the application and network policies in your environment. For information about how SiteScope monitors connect to remote systems, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586 and "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

You can also check for other information relating to monitoring remote servers in the HP Software Self-solve knowledge base (http://h20230.www2.hp.com/selfsolve/documents). To enter the knowledge base, you must log on with your HP Passport ID.

Monitoring Group Dependencies

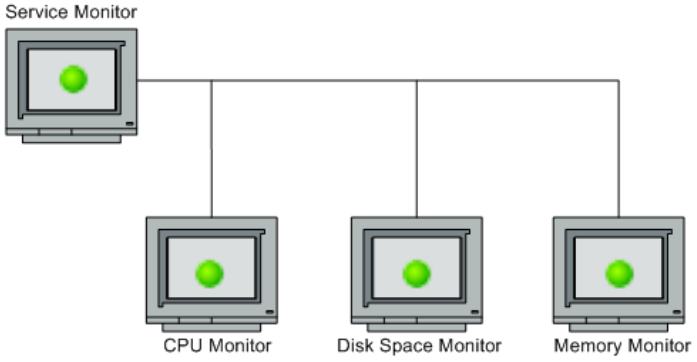
To prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system, select one monitor to check the basic availability of the system and then create other monitors that perform more detailed tests of that system. This creates a dependency relationship that enables you to make the running of a monitor group dependent on the status of a selected monitor.

For information about configuring dependency settings, see "Depends on" and "Depends condition" on page 456.

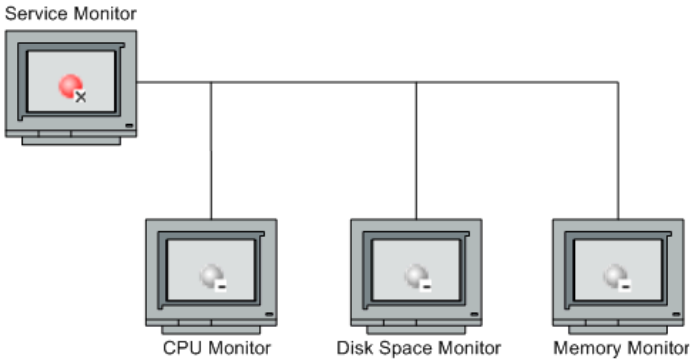
This section contains the following topics:

Depends On

You use this option to make the running of this monitor dependent on the status of another monitor. This can be used to prevent redundant alerting from multiple monitors that are monitoring different aspects of a single system. You can create a simple system monitor to check the basic availability or heartbeat of a system and then create other monitors that perform more detailed tests of that system. The figure below shows an example dependency relationship where three system monitors have been made dependent on a Service Monitor instance.



The detailed test monitors can be made dependent on the status of the heartbeat monitor by selecting that monitor. This means the dependent monitors run as long as the dependency condition is satisfied. If the heartbeat monitor detects that the target system has become unavailable, the dependency relationship automatically disables the other monitors. This has the effect of disabling any alerts that would have been generated by those monitors. The figure below shows the example monitors are disabled because the monitor on which they depend is reporting an error condition.



By default, no dependency is set for a monitor instance. To make the running of the monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the required monitor. To remove dependence on a monitor, clear the required check box.

Depends Condition

If you choose to make a monitor dependent on the status of another monitor (by using the **Depends on** setting), you use this option to select the status category or condition that the **Depends on** monitor should have for the current monitor to run normally.

The status categories include:

- Good
- Error
- Available
- Unavailable

The monitor being configured is run normally as long as the monitor selected in the **Depends on** box reports the condition selected in this box. If you have selected **Unavailable** and the **Depends on** monitor reports this status, the current monitors are not disabled.

For example, by selecting Good, this monitor is only enabled as long as the monitor selected in the **Depends on** box reports a status of Good. The current monitor is automatically disabled if the monitor selected in the **Depends on** box reports a category or condition other than the condition selected for this setting. See the examples for the Depends On setting.

Setting Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status is based on the results or measurements returned by the monitor action on the target system as compared to the thresholds set for the monitor.

You can set status threshold criteria for each monitor instance to determine an **Error** status, a **Warning** status, and a **Good** status. Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement value that you may specify. The parameter and the value depend on the monitor type. For example, the measurement parameter for a CPU monitor is CPU utilization (%). To indicate data volatility, where current monitor readings significantly deviate from monitor previous runs, set status thresholds using a baseline. For details, see "Setting Status Thresholds Using a Baseline" on page 405.

You can set up one or more status threshold criteria for each status condition. Most monitor types include one default setting for each of the three status conditions. Default thresholds of the monitor are displayed when you first configure the monitor.

In addition, for dynamic (VMware Host) monitors, you can display thresholds for all regular expression patterns that are translated to actual current counters. Patterns enable the monitor to automatically configure itself with counters on the relevant dynamic environment components. For more details, see "VMware Host Monitors Overview" in *Monitor Reference*.

For details on configuring monitor status thresholds, see "Threshold Settings" on page 457.

This section contains the following topics:

Scheduling

You can select a schedule to determine the status of the monitor instance if you want to define when to check the monitor run result against the threshold. This is useful if you want to restrict checking the monitor run results against the threshold to certain days or hours only. For example, you may want the monitor status to be based on results gathered during business hours only. At times outside the threshold schedule period, the monitor is assigned the predefined status in the **Default status** box. By default, monitor run results are checked against the threshold on an **every day, all day** schedule.

Availability

When the monitor is not available, it is assigned a status that is based on the user definition in the **If Unavailable** drop-down list. A monitor can have a state of **Unavailable** as well as a status of **Good**, **Warning**, or **Error**. Alerts are triggered according to availability, status, or both availability and status.

Baseline Thresholds

Instead of setting logic conditions manually in the threshold settings for each monitor instance, you can have SiteScope calculate thresholds for one or more monitor instances using a baseline. For information about this topic, see "Setting Status Thresholds Using a Baseline" on page 405.

Threshold Status Impact

A change of status signals an event and acts as a trigger for alerts associated with the monitor or the group to which the monitor belongs. For example, if the monitor detects that the system has become unavailable, the status change from **Good** to **Error** is used to trigger an alert on error.

A change of status may also affect the state of a dependency between monitors. For example, a monitor that detects a change that results in an **Error** status may be a trigger to disable one or more other monitors that are dependent on the system. For information about dependency settings, see "Monitoring Group Dependencies" on page 397.

The threshold setting also affects the status of the monitor in the SiteScope Dashboard. When viewing SiteScope data in the Current Status tab of Dashboard, you can drill down in the monitor tree to view monitor and measurement status and availability. The status is displayed by color and a status icon in the SiteScope Dashboard. For information on measurement status and availability in the Dashboard user interface, see "Status and Availability Levels" on page 1304.

Multiple Thresholds

The individual threshold criteria results are combined as logical **OR** relationships when more than one threshold condition is defined for any of the three settings. When one or more of the conditions (for example when two conditions for **Error if** setting) are met for a status setting the monitor status is set to the corresponding status condition. If status conditions are met for more than one status condition setting the status of the monitor is set to the highest valued status condition.

For example, if one condition selected as **Error if** and another condition selected as **Warning if** are both met, the status would be reported as an **Error**, with **Error** being the highest value, **Warning** the next highest and **Good** the lowest value.

SiteScope Metrics Assigned to Indicators

When SiteScope is reporting data to BSM, indicators provide a more detailed view of the health of a configuration item (CI). For details on understanding indicators, see "Health Indicators, KPIs, and KPI Domains" in *Service Health* in the HP Business Service Management Documentation Library.

When configuring thresholds for a monitor metric, monitors that have a defined topology and a default mapping have an indicator state and severity value assigned to the metric status by default.

- Every indicator can have several states. For example, when measuring CPU Load, the indicator state might be Bottlenecked or Busy, whereas when measuring Memory Load, the indicator state might be Paging or Starving for Memory.
- Indicator severity is the severity corresponding to the indicator state. The available indicator severity levels are Critical, Major, Minor, Warning, Normal, and Unknown.

Indicator states are assigned to the metric status according to the closest available severity that exists in the states for the indicator associated with the metric. The selected severity is shown in the SiteScope threshold. For example, when measuring percent used on a Memory monitor, the metric is mapped to Major severity in the **Error** threshold, since Critical severity is not available for the Memory Load indicator. When measuring round trip time on a Ping monitor, the closest severity level in the **Warning** threshold is Major, since the Minor severity level does not exist for this indicator state. The **Good** threshold is always mapped to the Normal severity level.

The association between the indicator state and severity cannot be changed on the local SiteScope server.

If you select a different indicator mapping in the HP Integration Settings pane for the monitor, the indicator state and severity values are updated in the Threshold Settings.

Note: If the **Indicator State and Severity** box is empty, the metric is not colored in Service Health, except for **always (default)** which is automatically assigned.

The default indicator assignments (mappings) are stored in the Indicator Assignment Settings in SAM Admin. For details, see "Indicator Assignment Settings" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

When there is a change to an assignment in the Indicator Assignment Settings, SiteScope detects the change and downloads the updated assignments. If indicator assignments have been changed on a local SiteScope server, these assignments are not overridden by the Indicator Assignment Settings. This includes indicator states where the state selected in the user interface is the same as the default value.

Note:

- If overlapping thresholds have been set (for example, Error if cpu utilization > 80% and Error if cpu utilization > 90%), the indicator state and severity value that is mapped to the closest threshold value is sent. In this example, if the actual metric value is 95%, then the indicator value that is mapped to Error if cpu utilization > 90% is sent. This is applicable only to thresholds where the values are numeric.
- Indicator state and severity are not displayed in SiteScope reports.

Setting Status Thresholds Using a Baseline

Baseline data is gathered from monitor performance metrics over a period of time and is used to provide a comparison for establishing acceptable or expected threshold ranges.

When the monitor's performance exceeds that range by some value (or does not reach that range, for example, in the case of Free Disk Space), the monitor can signal an error or warning. The acceptable threshold range of a monitor is determined by how far the current performance is from the baseline. Baselines enable you to understand how your applications typically perform and determine whether a performance problem is an isolated incident or a sign of a significant downward performance trend.

For details on this task, see "How to Set Monitor Thresholds Using a Baseline" on page 418.

This section contains the following topics:

Calculating the Baseline

To enable SiteScope to begin calculating baselines, you select the groups, monitors, or both, to be used for collecting baseline data. You can also select the schedule ranges used for collecting baseline threshold data. This enables you to restrict to certain days or hours of the week the periods during which SiteScope collects data for the baseline calculation. For example, you may want the monitor status to be based on results gathered during peak business hours only.

You can also select the adherence level used for determining the extent to which values for the baseline calculation affect the threshold values and set threshold boundaries for all monitor measurements. For details, see "Setting the Baseline Adherence Level" on page 409 and "Understanding the Good and Error Boundaries" on page 409.

The baseline engine calculates the baseline for each schedule using measurements collected from the monitors during the data collection period. SiteScope uses a percentile algorithm in the baseline calculation, in which a percentile value is used to determine the value of the baseline. For details on how baseline thresholds are calculated, see "Understanding Baseline Threshold Values" on page 411.

Activating the Baseline

After the baseline is calculated, you can review a summary of calculated monitors and analyze the baseline data in the Activate Baseline dialog box. The dialog box lists all the monitor instances for which a baseline was calculated, the date of the baseline calculation, and the reduction in the number of error and warning statuses that would have been generated for a monitor if the baseline thresholds were applied. If SiteScope is unable to calculate a baseline for a monitor, it lists a reason for calculation failure.

You can also view a graph that displays the current thresholds, the baseline thresholds, and historic data of all baseline-related monitor measurements over a 24-hour time period for each monitor measurement. The graph includes an annotation tool that enables you to annotate a snapshot of the graph you are viewing, to highlight important areas. You can save, print, or email an annotation graph. For user interface details, see "Annotation Tool" on page 1550.

After reviewing the baseline data, you can activate baseline threshold configuration. This applies the baseline values to the thresholds for the selected monitors. You can also activate the baseline for monitors that failed for the reason **Insufficient data** by using the limited measurement samples that were collected.

Before activating the baseline threshold, you should consider the option to save the current monitor configuration, because you cannot undo threshold configuration changes after the baseline has been activated.

When the baseline is activated, the baseline thresholds are displayed in the Threshold Settings area for each monitor. The baseline value is recalculated each day according to the history samples collected for the measurement and the current day's readings, and the baseline threshold values are recalculated and updated accordingly.

At any time, you can create a baseline summary report showing the baseline status and baseline status description for each monitor in the selected context.

Notes and Limitations

- Only an administrator in SiteScope, or a user granted **Edit monitors** permissions can use the baseline feature to set monitor thresholds, and only for the monitors that are in the users allowed groups list. Any user can view the Baseline Status Report regardless of edit permissions.
- You cannot add or delete thresholds or measurements, or copy or move monitors during the baseline calculation process (up until the point that the monitor baseline is activated).
- If you add, edit, or delete threshold measurements from browsable monitors after the baseline is activated for a monitor, the monitor needs to be recalculated and reactivated as a baseline monitor.
- Baseline thresholds are not copied or moved along with the other group or monitor objects when copying or moving a group or monitor with an activated baseline.
- If SiteScope is restarted before the remove baseline process is complete, the process is not continued after the restart, and you must run the remove baseline process again.

- If SiteScope is restarted before the baseline calculation or activation process is complete, it automatically continues the process after the restart. Monitors with any other baseline status (**Calculated, not activated**; **Activation failed**; **Calculation failed**; **Baseline activated**) are not affected by the restart.
- Before the baseline is calculated, the monitors should be enabled and permitted to run for a period long enough for SiteScope to accumulate sufficient data to calculate the baseline. This period depends on the **Minimum number of days required for baselining** and **Minimum number of samples required for baselining** settings in the Infrastructure Preferences. For details, see "Baseline Settings" on page 735. The baseline can still be calculated and activated even if the monitor has insufficient data, although the calculation may not be accurate.
- After you define a set of counters for a browsable monitor and the monitor runs with these counters for some time, if you later change the counters (for example, remove existing counters and/or add new counters), and then you attempt to calculate baseline, the calculation results may be incorrect. This can occur because old data, possibly for counters that no longer exist, interferes with the new data. The calculation may also be incorrect for counters that have not changed since the monitor was created. To avoid this problem, you should not make any changes to a monitor's browsable counters during the minimum number of days period required for calculating the baseline.
- You can change threshold related properties using Global Search and Replace, regardless of whether the threshold was created using a baseline or manually. However, you cannot activate a baseline threshold for a monitor using Global Search and Replace.
- During the baseline calculation and after the baseline is activated, only certain baseline threshold changes are supported. The same restrictions apply when you change threshold related properties using Global Search and Replace. For details on the threshold changes that are allowed, see "Changing Threshold Settings" on page 465.
- Memory consumption increases for each monitor threshold set using a baseline. To reduce memory consumption, you can set the **Interval for saving accumulated baseline data to disk** settings in the Baseline Settings. For details, see "Baseline Settings" on page 735.

Setting the Baseline Adherence Level

You can select the baseline adherence level used for determining the threshold value. This is the extent to which values for the baseline calculation affect the threshold values for all monitor measurements. You can select **High adherence**, **Medium adherence**, or **Low adherence**. The higher the adherence level, the closer the threshold range is to the monitor measurement baseline values. Conversely, the lower the adherence level, the further the threshold range is from the monitor measurement baseline values.

In addition to selecting the adherence level, you can also fine-tune the adherence level for individual monitor measurements by configuring adherence percentiles separately for each monitor measurement. Adherence levels are based on adherence percentiles—a measurement value that determines when a measurement is in error or warning. For browsable monitor measurements, you can configure only one set of adherence percentiles that is used by all browsable monitors.

To manually fine-tune the adherence level, you should understand how the threshold values are created. For details on this topic, see "Understanding Baseline Threshold Values" on page 411.

Understanding the Good and Error Boundaries

Configuring good and error boundaries is useful to avoid setting off errors and warnings unnecessarily when using baseline thresholds. You can manually set a good boundary for each monitor measurement and the browsable monitor counters. SiteScope automatically configures the error boundary for each monitor measurement.

Note: To set good boundaries, it is important to understand how baseline threshold values are created. For details on this topic, see "Understanding Baseline Threshold Values" on page 411.

Good Boundary

This is the value of a measurement that is not considered to be in error status, even though according to existing baseline percentiles it should report an error. For example, consider a low load system where CPU utilization measurements are constantly below 3%. Based on these measurements, SiteScope might calculate a baseline threshold with a 5% error threshold. Because this is not an accurate measure of CPU load error, you may want to define 70% CPU utilization as the good boundary to avoid generating false errors. Provided CPU utilization remains below this limit (even though it is above the baseline error threshold), the monitor is not in error status.

You manually set the Good Boundary in the Fine Tune Adherence Levels /Set Boundary dialog box. For user interface details, see "Fine-Tune Adherence Levels/Set Boundary Dialog Box" on page 497.

Error Boundary

This is the value of a measurement that is considered to be in error status, even though according to existing baseline percentiles it should not report an error. This can occur when a measurement value grows slowly over a period of time, for example, due to a slow memory leak. Because the baseline threshold is recalculated and updated every day as the measurement average increases, the measurement value does not cross the new threshold.

To overcome this problem, SiteScope automatically sets the error boundary for each monitor measurement. It does this by setting a limit that triggers errors when monitor measurements exceed a specified value, regardless of the baseline. For example, if SiteScope sets an error boundary of 80% CPU utilization, values over 80% CPU utilization are in error status even if the calculated baseline error threshold is not exceeded.

For information on how the error boundary is calculated, see "How SiteScope Calculates the Error Boundary" on page 412.

Understanding Baseline Threshold Values

To help you fine-tune the percentile value used in the baseline calculation at each adherence level and to set the error and good boundaries (for details, see "Understanding the Good and Error Boundaries" on page 409), it is important to understand:

- The types of threshold values.
- How they are applied to measurements.
- How measurements are used to calculate baseline thresholds and boundaries.

Baseline thresholds are added or updated dynamically to the monitor configuration for each measurement the monitor had before the baseline was calculated. Baseline thresholds are added for each schedule selected for collecting baseline data.

In general, there are two types of thresholds: baseline thresholds and static thresholds. Baseline thresholds have a percentile value that is used to determine when a measurement is in error or warning status, while static thresholds have an actual fixed value. Baseline threshold measurements have a condition of either >= or <= depending on the direction of the measurement.

Baseline thresholds are changed, added, or deleted on measurements provided the following two conditions are met:

- The measurement can be used in the baseline calculation. To be used in the baseline calculation, a measurement must be numeric and it must have a direction. An example of a measurement that cannot be used in the baseline calculation is a URL 404 error code (it is numeric, but it has no direction).
- The measurement has a static threshold defined for any schedule and any status category (Good, Warning, Error) prior to the baseline calculation.

Measurements that do not adhere to these conditions are not affected (in terms of the thresholds defined on them), and a baseline is not calculated for these measurements.

How SiteScope Calculates Thresholds

When SiteScope calculates the baseline, it creates a percentile value for each baselinable threshold measurement for each schedule. SiteScope makes an adjustment for extreme measurements by discarding, by default, 2% of the most extreme samples (considered "noise" measurements), and calculates the percentiles on the remaining measurements. For example, if most monitor run results on a server show CPU utilization of no more than 20% and one peak value of 50%, the peak value is not used to determine the baseline. You can change the percentage of discarded measurement samples in the Baseline Settings.

The baseline engine uses a sliding-window approach to calculate thresholds. This means that newer data samples have more influence on the baseline calculation than older samples, and that after a period of time (by default 30 days), the historic data becomes obsolete. You can set the number of days to include in the calculation in the Baseline Settings.

For information about configuring Baseline Settings in the Infrastructure Preferences, see "Baseline Settings" on page 735.

How SiteScope Calculates the Error Boundary

SiteScope uses the percentile value to create an error boundary for each measurement. This is the value of a measurement that is considered to be in error status, even though according to existing baseline percentiles it should not report an error. For details, see "Error Boundary" on page 410.

SiteScope calculates the error boundary in one of the following ways:

- If the measurement has a static error threshold for the specific schedule, the percentile value of the baseline threshold is calculated into an actual value and this value is then compared to the value of the static threshold as follows:
  - If the static error threshold value is more extreme than the baseline threshold value, the static error threshold value is used as the error threshold boundary for that measurement.

    Example: If the static error threshold is 100% CPU utilization and the computed baseline threshold is 67% CPU utilization, the static error threshold value (100% CPU utilization) is used as the error boundary.

- If the baseline threshold value is more extreme than the static error threshold value, then the offset value is used. The offset is a percentage value that SiteScope adds to the baseline threshold value (or subtracts from, depending on the direction of the measurement), and the resulting value is used as the error boundary for that measurement. You can determine the offset value in the Baseline Settings area of Infrastructure Preferences.

  Example: If the static error threshold for a schedule is 60% CPU utilization and the computed baseline threshold value is 65% CPU utilization, the error boundary is calculated as:
  65% CPU utilization * 130% (using the default offset value of 0.3) = 84.5% CPU utilization.

- If there is no error threshold value for the measurement with the specific schedule prior to calculating the baseline (the measurement has a warning or good threshold value but no error threshold value), and the **Automatically create an error boundary if no error thresholds are defined** option is selected in the Baseline Settings, the percentile value of the baseline threshold is calculated into an actual value and the offset value is added to/subtracted from the baseline threshold value (depending on the direction of the measurement). The resulting value is used as the error boundary for the measurement.

Note: An error boundary is not created if:

- There is no error threshold value for the measurement with the specific schedule prior to calculating the baseline (for example, the measurement has a warning or good threshold value but no error threshold value), and
- The **Automatically create an error boundary if no error thresholds are defined** option is not selected.

For details on defining the offset value and automating error boundary creation, see "Baseline Settings" on page 735.

Tasks

How to Deploy a Monitor

This task describes the steps involved in deploying a monitor.

1 Prerequisites

Check if there are setup requirements and user permissions that need to be obtained for the monitor before configuring the monitor. For details, see the help for the specific monitor in the *Monitor Reference* guide.

Note:

- Monitors must be created in a group in the monitor tree. For task details, see "Create SiteScope groups and subgroups" on page 384.
- To enable SiteScope to monitor data on remote servers, you must configure remote servers. For details on configuring a Windows remote server, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586. For details on configuring a UNIX remote server, see "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

---

2 Create monitor instances

a To create a new monitor instance, right-click the group into which you want to add the monitor instance, and select **New** > **Monitor**. For user interface details, see "New Monitor Dialog Box" on page 444.

Note: Alternatively, you can create a new monitor instance by copying or moving existing monitor instances to the group in the monitor view. For details, see "Copying and Moving SiteScope Objects" on page 69.

---

b Select the monitor you want to add from the New Monitor dialog box, and configure the settings for the specific monitor. For a description of the monitor settings, see the help for the specific monitor in *Monitor Reference*.

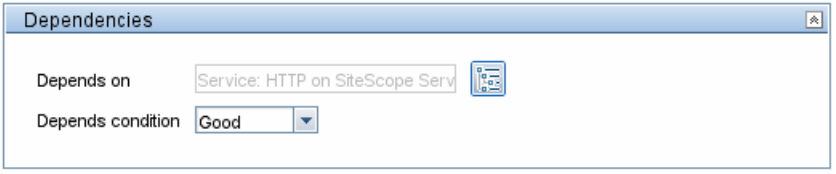
c You can configure other properties that affect the monitor. For example:

➤ In the **Monitor Run Settings** tab, you can set how often SiteScope attempts to run the action defined for the monitor instance. You can also set the range schedule if you want the monitor to run on certain days or on a fixed schedule. For user interface details, see "Monitor Run Settings" on page 451.

➤ In the **Dependencies** tab, you can set monitor dependencies to make the running of this monitor dependent on the status of another monitor. For user interface details, see "Dependencies" on page 454.

Example:

The monitor being configured is run normally as long as the monitor selected in the **Depends on** box reports the condition selected in the **Depends condition** box. In this example, the monitor being configured is enabled only when the **Service** monitor reports a status of **Good**.

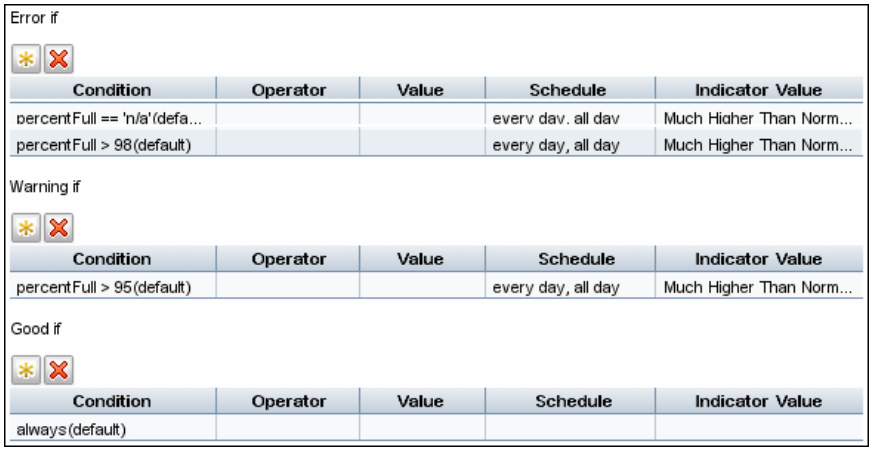


➤ In the **Threshold Settings** tab, you can manually set logic conditions that determine the reported status of each monitor instance. For user interface details, see "Threshold Settings" on page 457.

Alternatively, you can set thresholds for one or multiple monitors using a baseline. For task details, see "How to Set Monitor Thresholds Using a Baseline" on page 418.

Example:

The following shows the default threshold settings for a disk space monitor:



Disk space of less than 95 percent full results in a good status; disk space greater than 95 percent full but lower than 98 percent full results in a warning status; disk space greater than 98 percent full or "n/a" results in an error status.

➤ For details of the other common monitor properties, see "Common Monitor Settings" on page 447.

3 Set up monitor alerts - optional

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

To create an alert for the monitor, right-click the monitor and select **New > Alert**. For each alert scheme, you can create one or more alert actions. In the New Alert dialog box, click **New Alert Action** to start the Alert Action wizard.

For task details, see "How to Configure an Alert" on page 1443.

4 Set up monitor reports - optional

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

To create a report for the monitor, right-click the monitor and click **Reports**. Select a report type and configure the report settings.

For task details, see "How to Create a Report" on page 1508.

5 Results

The monitor is added to the monitor group in the monitor tree with the configuration settings that you specified displayed in the Properties tab.

How to Set Monitor Thresholds Using a Baseline

This task describes the steps involved in setting monitor thresholds using a baseline.

This task includes the following steps:

1 Prerequisites

Before calculating a baseline for a monitor, make sure that the monitor is enabled and has run for a period long enough for SiteScope to accumulate sufficient data to calculate the baseline. This period depends on the minimum number of days and samples required to calculate the baseline which you configure in the Baseline Settings. For user interface details, see "Baseline Settings" on page 735.

Note: The baseline can still be calculated and activated even if the monitor has insufficient data, although the calculation may not be accurate.

---

2 Configure baseline setting preferences - optional

You can view and define the values of global SiteScope baseline settings in Infrastructure Preferences. This includes calculation and activation priority settings, the number of days of historical data to include in baseline calculations, and the offset for calculating the error boundary.

For user interface details, see "Baseline Settings" on page 735.

3 Calculate the baseline

Define thresholds on the monitor measurements for which the baseline should be calculated.

a Select the monitor instances you want to baseline. For user interface details, see "Select Monitors for Baseline Calculation" on page 494.

b Select one or more schedule ranges to be used for collecting baseline data, or accept the default schedule (**every day, all day**). For user interface details, see "Schedule" on page 494.

c Select the global baseline adherence level that is used for determining the extent to which values for the baseline calculation affect the threshold values for all monitor measurements. For user interface details, see "Adherence Level" on page 495.

d Additionally, you can click the **Fine-Tune Adherence Levels/Set Boundary** button to:

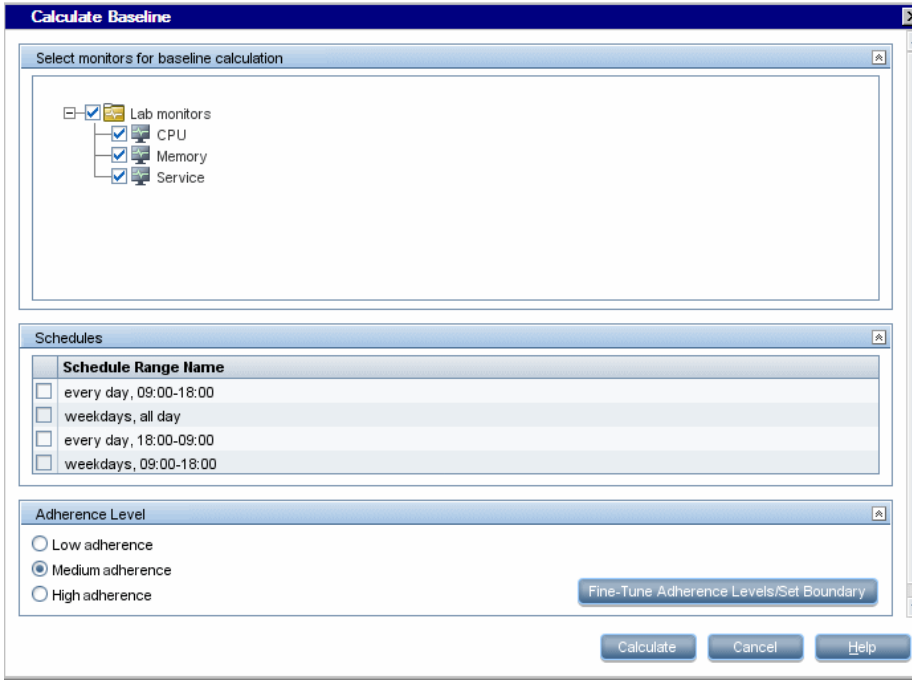
- Individually fine-tune the baseline adherence level for any monitor measurement.
- Define a good boundary for each monitor measurement. A measurement within this boundary is not in error status, even though it should report an error according to existing baseline percentiles.

For user interface details, see "Configure Adherence Percentiles" on page 497.

e Click **Calculate** to perform the baseline threshold calculation.

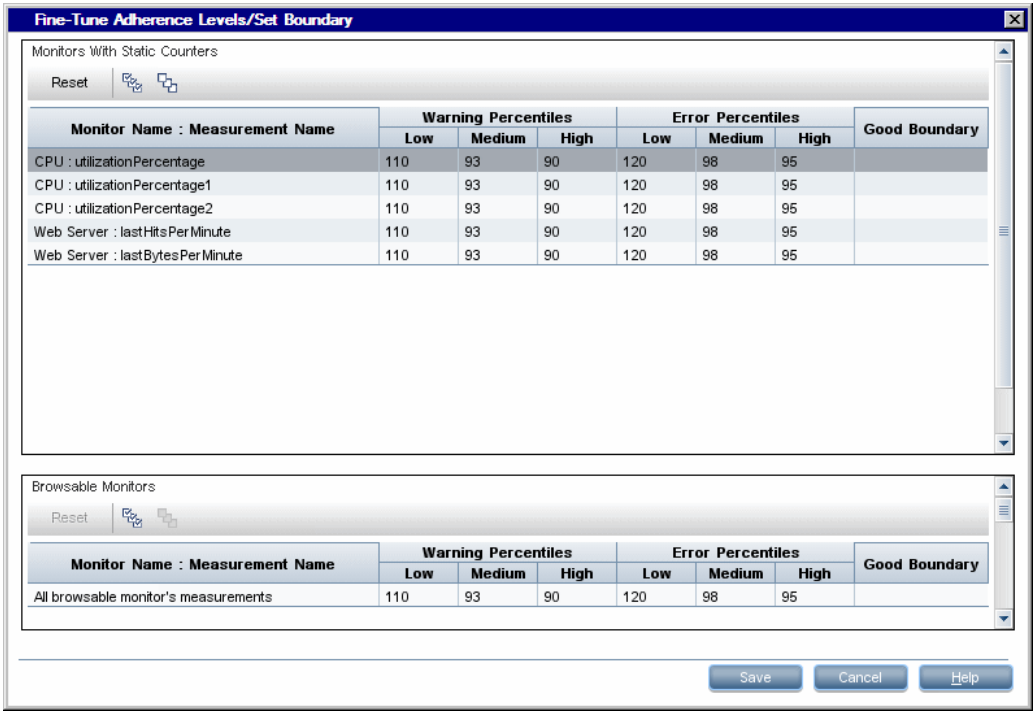
Example:

Example of the Calculate Baseline dialog box.



Note: Only those monitors that the user is eligible to see according to their user permissions are displayed.

Example of the Fine-Tune Adherence Levels/Set Boundary dialog box.

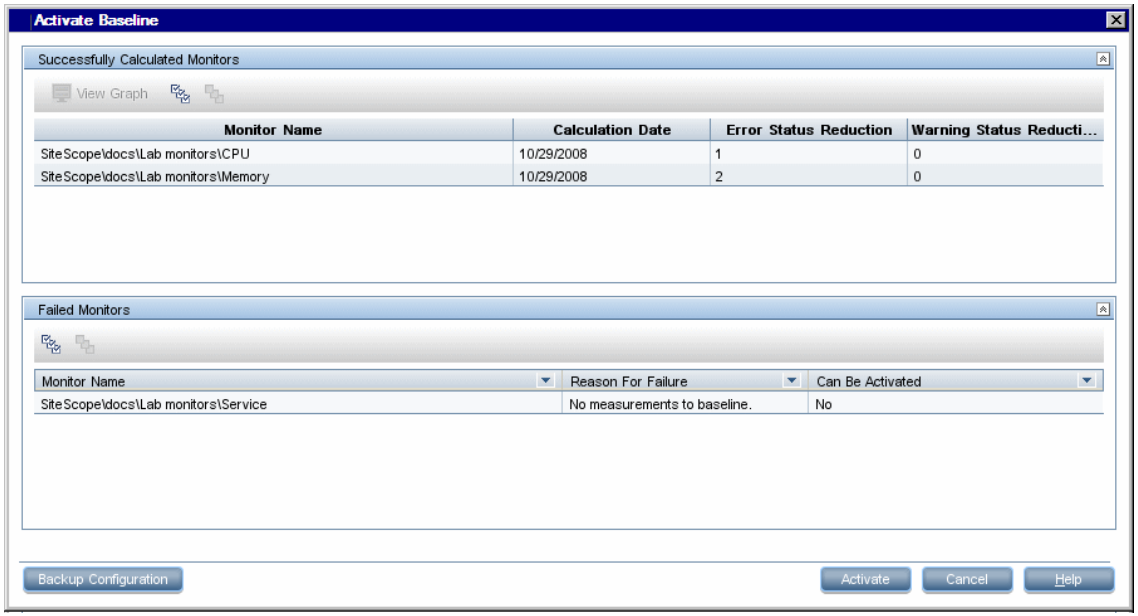


4 Review the baseline settings

Review the summary of calculated monitors and baseline data in the Activate Baseline dialog box. Only the monitors that the user is eligible to see according to their user permissions are displayed.

For user interface details, see "Activate Baseline Dialog Box" on page 499.

Example:



Note: Only those monitors that the user is eligible to see according to their user permissions are displayed.

---

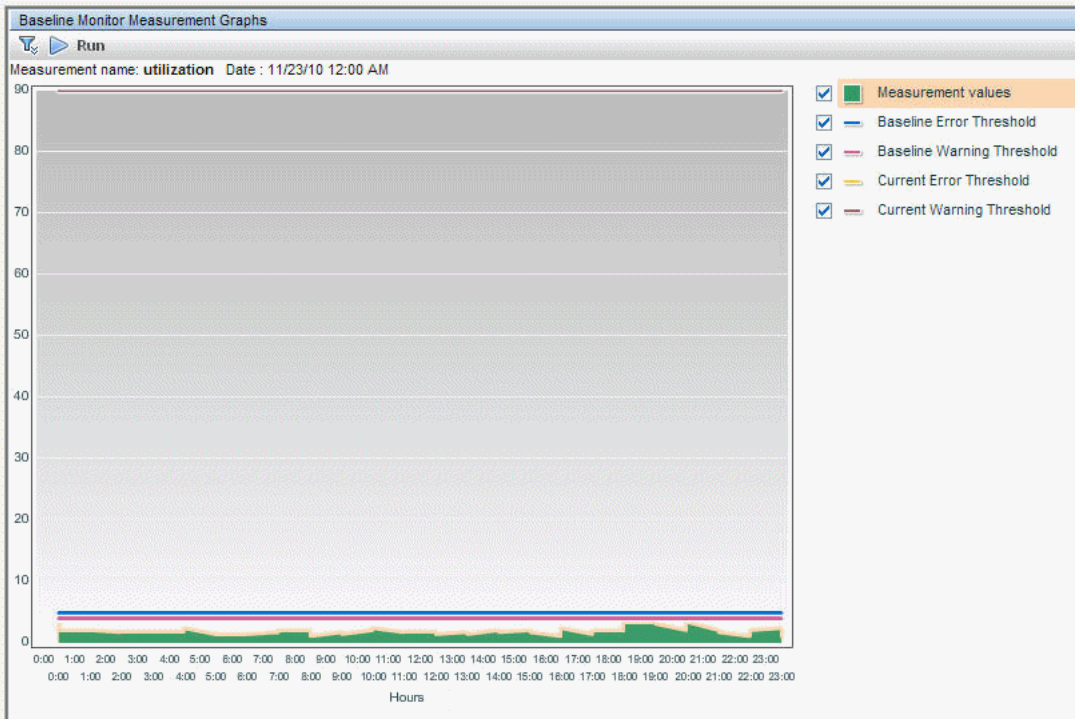
5 View the baseline monitor measurements graphs

You can view a graphical display of each monitor's baselined measurements to analyze the baseline data for a selected day. You can also use the annotation tool to create a snapshot of the graph you are viewing and highlight important areas.

For user interface details, see "Baseline Monitor Measurement Graphs Dialog Box" on page 504.

Note: The data displayed in the graphs is an aggregate of the measurement data and as such, the time periods may not accurately reflect the time the data was collected.

Example:



6 Activate the baseline settings

Select the monitors for which you want to set thresholds using a baseline, and click **Activate**. You can select all monitors with a successfully calculated baseline, and those that failed with the reason **Insufficient data** (indicated by **Yes** in the **Can Be Activated** column). The monitor thresholds are configured according to the baseline calculation, and are set to change status when the thresholds settings are exceeded.

For user interface details, see "Activate Baseline Dialog Box" on page 499.

Note: If you want to revert to the current monitor threshold configuration, select the option to save the current monitor configuration before activating the baseline configuration.

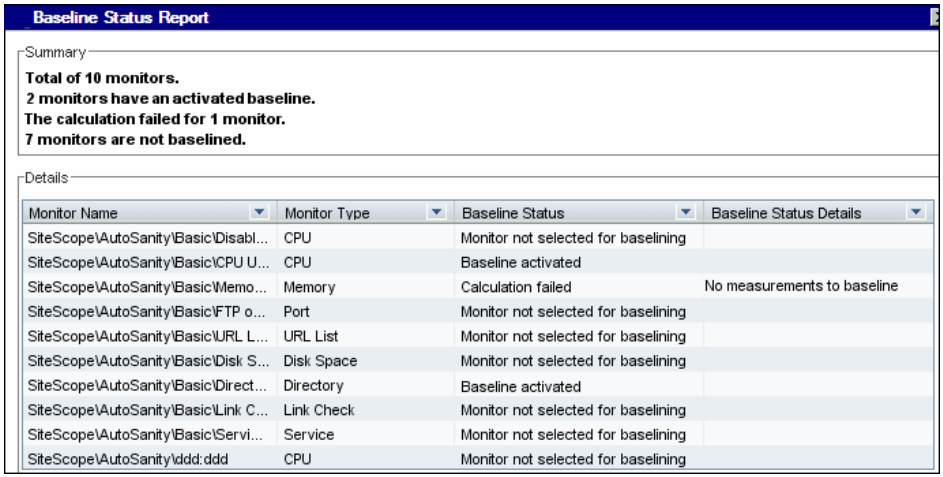
---

7 View baseline properties in the Baseline Status Report

You can create an ad hoc report showing information about each monitor in the selected context, including each monitor's baseline status and baseline status description. For user interface details, see "Baseline Status Report" on page 509.

You can also track the baseline status for a monitor in the monitor's Baseline Settings. For user interface details, see "Baseline Settings" on page 485.

Example:



Baseline Status Report

Summary

Total of 10 monitors.
2 monitors have an activated baseline.
The calculation failed for 1 monitor.
7 monitors are not baselined.

Details

Monitor Name	Monitor Type	Baseline Status	Baseline Status Details
SiteScope\AutoSanity\Basic\Disabl...	CPU	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\CPU U...	CPU	Baseline activated	
SiteScope\AutoSanity\Basic\Memo...	Memory	Calculation failed	No measurements to baseline
SiteScope\AutoSanity\Basic\FTP o...	Port	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\URL L...	URL List	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\Disk S...	Disk Space	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\Direct...	Directory	Baseline activated	
SiteScope\AutoSanity\Basic\Link C...	Link Check	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\Servi...	Service	Monitor not selected for baselining	
SiteScope\AutoSanity\ddd:ddd	CPU	Monitor not selected for baselining	

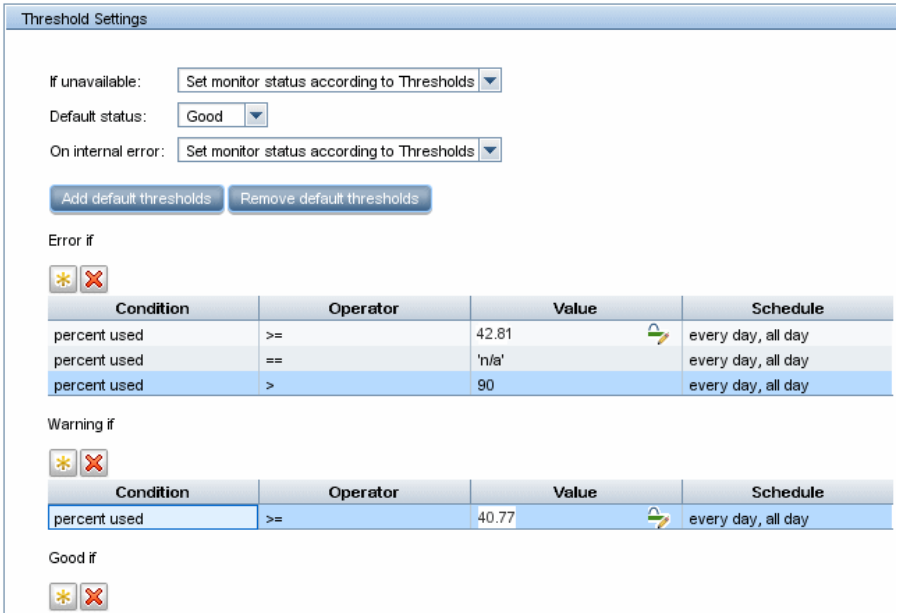
8 View and modify baseline thresholds

In the Threshold Settings, you can view the baseline thresholds and manually fine-tune the thresholds by changing the percentile value from which the threshold value is derived.

For user interface details, see "Threshold Settings" on page 457.

Example:

In the example, the Error if percent used threshold value is >= 42.81 and the Warning if percent used threshold value is >= 40.77 (both these values are non-editable). To change the threshold values, you must change the percentile value from which the threshold values are derived. To help you understand what the new threshold value is after you change the percentile value, click the **Percentiles Table** button to open the percentile table that shows the threshold value that is mapped to each percentile range.



Note: The **Error if percent used (default)** > 90 threshold is the error boundary. This is the value of a measurement considered to be in error status, even though according to existing baseline percentiles it should not report an error. For example, if the baseline threshold were updated to **Error if percent used (%)** >= 96, all measurements greater than 90 are in error status, even if the calculated baseline error threshold of 96 is not exceeded. For details on this topic, see "Error Boundary" on page 410.

Reference

Monitor Categories List

This section displays the SiteScope monitors in each monitor category. For information about the usage and configuring each monitor type, see the monitor type in the *Monitor Reference* guide.

- "Application Monitors" on page 428
- "Database Monitors" on page 430
- "Generic Monitors" on page 430
- "Integration Monitors" on page 430
- "Media Monitors" on page 431
- "Network Monitors" on page 431
- "Server Monitors" on page 432
- "Web Transaction Monitors" on page 432
- "Virtualization and Cloud Monitors" on page 433

Application Monitors

- Active Directory Replication Monitor
- Apache Server Monitor
- BroadVision Application Server Monitor
- Check Point Monitor
- Cisco Works Monitor
- Citrix Monitor
- ColdFusion Server Monitor
- COM+ Server
- F5 Big-IP Monitor

- Microsoft ASP Server Monitor
- Microsoft Exchange 2007/2010 Monitor
- Microsoft Exchange 2003 Mailbox Monitor
- Microsoft Exchange 5.5 Message Traffic Monitor
- Microsoft Exchange 2000/2003/2007 Message Traffic Monitor
- Microsoft Exchange 2003 Public Folder Monitor
- Microsoft IIS Server Monitor
- News Monitor
- Oracle 9i Application Server Monitor
- Oracle 10g Application Server Monitor
- Radius Monitor
- SAP CCMS Monitor
- SAP CCMS Alerts Monitor
- SAP Java Web Application Server Monitor
- SAP Performance Monitor
- SAP Work Processes Monitor
- Siebel Application Server Monitor
- Siebel Log File Monitor
- Siebel Web Server Monitor
- SunONE Web Server Monitor
- Tuxedo Monitor
- UDDI Monitor
- WebLogic Application Server Monitor
- WebSphere Application Server Monitor
- WebSphere MQ Status Monitor
- WebSphere Performance Servlet Monitor

Database Monitors

- DB2 8.x and 9.x Monitor
- Database Counter Monitor
- Database Query Monitor‘
- LDAP Monitor
- Microsoft SQL Server Monitor
- Oracle Database Monitor
- Sybase Monitor

Generic Monitors

- Composite Monitor
- Directory Monitor
- File Monitor
- JMX Monitor
- Log File Monitor
- Multi Log File Monitor
- Script Monitor
- Web Service Monitor
- XML Metrics Monitor

Integration Monitors

- HP OM Event Monitor
- HP Service Manager Monitor
- NetScout Event Monitor
- Technology Database Integration Monitor
- Technology Log File Integration Monitor
- Technology SNMP Trap Integration Monitor
- Technology Web Service Integration Monitor

Media Monitors

- Microsoft A/V Conferencing Server Monitor
- Microsoft Archiving Server Monitor
- Microsoft Director Server Monitor
- Microsoft Edge Server Monitor
- Microsoft Front End Server Monitor
- Microsoft Mediation Server Monitor
- Microsoft Monitoring and CDR Server Monitor
- Microsoft Registrar Server Monitor
- Microsoft Windows Media Player Monitor
- Microsoft Windows Media Server Monitor
- Real Media Player Monitor
- Real Media Server Monitor

Network Monitors

- DHCP Monitor
- DNS Monitor
- FTP Monitor
- Formula Composite Monitor
- Mail Monitor
- MAPI Monitor
- Microsoft Windows Dial-up Monitor
- Network Bandwidth Monitor
- Ping Monitor
- Port Monitor
- SNMP Monitor

- SNMP Trap Monitor
- SNMP by MIB Monitor

Server Monitors

- Browsable Windows Performance Monitor
- CPU Monitor
- Disk Space Monitor
- HP iLO (Integrated Lights-Out) Monitor
- HP NonStop Event Log Monitor
- HP NonStop Resources Monitor
- IPMI Monitor
- Memory Monitor
- Microsoft Windows Event Log Monitor
- Microsoft Windows Performance Counter Monitor
- Microsoft Windows Resources Monitor
- Microsoft Windows Services State Monitor
- Service Monitor
- UNIX Resources Monitor
- Web Server Monitor

Web Transaction Monitors

- e-Business Transaction Monitor
- Link Check Transaction Monitor
- URL Monitor
- URL Content Monitor
- URL List Monitor
- URL Sequence Monitor
- Web Script Monitor

Virtualization and Cloud Monitors

- Amazon Web Services Monitor
- Microsoft Hyper-V Monitor
- Solaris Zones Monitor
- VMware Host CPU Monitor
- VMware Host Memory Monitor
- VMware Host Network Monitor
- VMware Host State Monitor
- VMware Host Storage Monitor
- VMware Performance Monitor

Monitors Supported in SiteScopes Installed on Windows Environments Only

The following lists the monitors that are supported in SiteScopes that are running on Windows versions only. Where relevant, the monitors can monitor remote servers running on any platform/operating system.

- MAPI Monitor
- Microsoft Exchange 2003 Mailbox Monitor
- Microsoft Exchange 2003 Public Folder Monitor
- Microsoft Exchange 2000/2003/2007 Message Traffic Monitor
- Microsoft Exchange 2007/2010 Monitor
- Microsoft Exchange 5.5 Message Traffic Monitor
- Microsoft Windows Dial-up Monitor
- Microsoft Windows Media Player Monitor
- Real Media Player Monitor
- Sybase Monitor

- Tuxedo Monitor
- Web Script Monitor

Monitors Supporting Windows Management Instrumentation (WMI)

The following lists the monitors that support the Windows Management Instrumentation (WMI) method for collecting data. WMI is a more secure communication method than NetBIOS for gathering management data from remote servers running on Windows servers.

- Citrix Monitor
- ColdFusion Server Monitor
- CPU Monitor
- Disk Space Monitor
- Memory Monitor
- Microsoft A/V Conferencing Server Monitor
- Microsoft Archiving Server Monitor
- Microsoft ASP Server Monitor
- Microsoft Director Server Monitor
- Microsoft Edge Server Monitor
- Microsoft Front End Server Monitor
- Microsoft Hyper-V Monitor
- Microsoft IIS Server Monitor
- Microsoft Mediation Server Monitor
- Microsoft Monitoring and CDR Server Monitor
- Microsoft Registrar Server Monitor
- Microsoft SQL Server Monitor
- Microsoft Windows Event Log Monitor

- Microsoft Windows Media Server Monitor
- Microsoft Windows Resources Monitor
- Microsoft Windows Services State Monitor
- Real Media Server Monitor
- Service Monitor

For details on how to configure the WMI service on the remote machine, see "Configure the WMI Service for Remote Monitoring" on page 596.

Ports Used for SiteScope Monitoring

The following table lists the network ports that are generally used for SiteScope monitoring. In many cases, alternate ports may be configured depending on the security requirements of your environment.

Monitor Type	Ports Used
Apache Server Monitor	Port which Apache Server Admin pages located. Configurable by using server configuration file.
BroadVision Application Server Monitor	Uses the Object Request Broker (ORB) port number for the BroadVision server you are trying to monitor.
Check Point Monitor	SNMP monitor. Default is port 161. This is configurable.
Cisco Works Monitor	Cisco Works resources are usually available by using port 161 or 162 (SNMP), depending on the configuration of the server.
Citrix Monitor	Ports 137, 138, and 139 (NetBIOS).
ColdFusion Server Monitor	Ports 137, 138, and 139 (NetBIOS).
CPU Monitor	For local CPU, no ports required. For CPUs on remote servers (Windows-based systems): ports 137, 138, and 139 (NetBIOS). For CPUs on remote servers (Solaris/Linux-based systems): ports 22 (SSH), 23 (telnet), or 513 (rlogin).
Database Query Monitor	This is configurable and depends on ODBC or JDBC driver and DB configuration.
DB2 8.x and 9.x Monitor	Default is port 50000. This is configurable.
DHCP Monitor	Default is port 68.

Monitor Type	Ports Used
Directory Monitor	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 Monitor	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 Monitor	Default is port 53.
F5 Big-IP Monitor	Uses SNMP. This is configurable.
File Monitor	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 Monitor	Default is port 21. This is configurable.
LDAP Monitor	The default is port 389. This is configurable.
Link Check Transaction Monitor	The default is port 80. This is configurable.
Log File Monitor	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Mail Monitor	Port 110 for POP3, port 25 for SMTP, port 143 for IMAP.

Monitor Type	Ports Used
MAPI Monitor	MAPI uses the Name Service Provider Interface (NSPI) on a dynamically assigned port higher than 1024 to perform client-directory lookup.
Memory Monitor	Ports 137, 138, and 139 (NetBIOS) for Windows based systems, ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Microsoft Archiving Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft A/V Conferencing Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft ASP Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft Director Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft Edge Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft Front End Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft Hyper-V Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft IIS Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft Mediation Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft Monitoring and CDR Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft Registrar Server Monitor	Windows Performance Counters over ports 137, 138, and 139 (NetBIOS).
Microsoft SQL Server Monitor	Ports 137, 138, and 139 (NetBIOS).

Monitor Type	Ports Used
Microsoft Windows Event Log Monitor	Ports 137, 138, and 139 (NetBIOS).
Microsoft Windows Media Player Monitor	Same port as media content to be monitored.
Microsoft Windows Media Server Monitor	Ports 137, 138, and 139 (NetBIOS).
Microsoft Windows Performance Counter Monitor	Ports 137, 138, and 139 (NetBIOS).
Microsoft Windows Resources Monitor	Ports 137, 138, and 139 (NetBIOS).
Network Bandwidth Monitor	No ports required; monitors only the local machine.
News Monitor	Default is port 144. This is configurable.
Oracle Database Monitor	This is configurable. Depends on target DB. Default is port 1521.
Oracle 9i Application Server Monitor/Oracle 10g Application Server Monitor	This is configurable. Port which Webcaching admin page located.
Ping Monitor	Default is port 7.
Port Monitor	Monitors any port.
Radius Monitor	Currently supports Password Authentication Procedure (PAP) authentication but not the Challenge Handshake Authentication Protocol (CHAP) or Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). The RADIUS servers must be configured to accept PAP requests. Default is port 1645. In recent changes to the RADIUS spec, this may be changed to 1812. The monitor is configurable.

Monitor Type	Ports Used
Real Media Player Monitor	Uses Real Media client on SiteScope box. Uses the port from which the media content is streamed (based on the URL).
Real Media Server Monitor	Ports 137, 138, and 139 (NetBIOS).
SAP CCMS Monitor	Uses SAP Client software (SAP Front End) to run certain SAP transactions. Therefore, same ports as SAP.
Script Monitor	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Service Monitor	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
SNMP Monitor	Default is port 161. This is configurable.
SNMP Trap Monitor	Uses port 162 for receiving traps. This is configurable.
SunONE Web Server Monitor	URL to the stats-xml file on the target SunONE server. The port is configurable.
Sybase Monitor	Monitor requires Sybase Central client on the machine where SiteScope is running to connect to the Adaptive Server Enterprise Monitor Server. Port number the same as Sybase client.
Tuxedo Monitor	The default port for the TUXEDO workstation listener is port 65535. This is configurable.
URL Monitor	Generally port number 80. This is configurable.
Web Server Monitor	Ports 137, 138, and 139 (NetBIOS) for Windows based systems. Ports 22 (SSH), 23 (telnet), or 513 (rlogin) for Solaris/Linux based systems.
Web Service Monitor	This is configurable.

Monitor Type	Ports Used
WebLogic Application Server Monitor	Oracle WebLogic Application Server monitor uses the Java JMX interface. Port is configurable.
WebSphere Application Server Monitor	Same port as the IBM WebSphere Administrator's Console.
WebSphere Performance Servlet Monitor	WebSphere Performance Servlet. Port is configurable.

Note: All monitors that support perfex—SiteScope's internal application that connects to Windows APIs—may use port 135, in addition to other ports.

List of Deprecated SiteScope Monitors

In recent versions of SiteScope, a number of monitors were deprecated and are no longer supported. The following table lists the deprecated monitors, and where available, the respective monitors that can replace them.

Deprecated Monitor	Recommended Alternative Monitor
Active Directory Performance	N/A
Asset	N/A
Astra Load Test	Web Script
DB2	DB2 8.x and 9.x
Dynamo	N/A
IPlanet Application Server	SunONE Web Server
IPlanet Server	SunONE Web Server
IPlanet Web Server	SunONE Web Server
Network	Network Bandwidth
Quick Test Pro	Web Script
RTSP	Real Media Player
SAP	SAP Performance
SAP Portal	SAP CCMS
SilverStream Server	N/A
WebLogic 5.x Application Server	N/A

For SiteScope upgrade purposes, you can check if the current configuration has any deprecated monitors using the End of Life Monitor Viewer. For details on using the End of Life Monitor Viewer, see "Using the End of Life Monitor Viewer" in the *HP SiteScope Deployment Guide* PDF.

For a list of deprecated Technology Integration monitors, see "List of Deprecated Integration Monitors" on page 541.

SiteScope Monitors User Interface

This section includes:

New Monitor Dialog Box

The New Monitor dialog box enables you to define a new monitor in a monitor group.

To access	Select the **Monitors** context. In the monitor tree, right-click a group and select **New** > **Monitor**.
Important information	➤ Monitors can be created only in a SiteScope group. ➤ You cannot delete a monitor if it has dependent alerts or reports at the container level. To delete a monitor with dependencies, you must remove the monitor from **Alert Targets** and **Report Targets** for each dependency, and then delete the monitor. You can delete monitors that have dependencies at the child level. ➤ The Monitor description field supports HTML tags (HTML version 3.2) including the most common tags for text styling, such as , <HR>, and <B>, and hyperlinks. It does not support JavaScript/iframes/frames or other advanced features. ➤ You can also use the SiteScope API when working with monitors. For details, see "Using the SiteScope Configuration API" on page 42.
Relevant tasks	"How to Deploy a Monitor" on page 414
See also	"Monitor Tree" on page 81

Main Settings

User interface elements are described below:

UI Element	Description
Quick Search	Enter a monitor name in the **Quick Search** box. You can select the following settings to help you with your search: ➤ **All.** Search for matches in all columns. ➤ **Monitor.** Search for matches in the Monitor column only. ➤ **Category.** Search for matches in the Category column only. ➤ **Case sensitive.** Search for matches that are case sensitive. ➤ **Case insensitive.** Search for matches that are not case sensitive. ➤ **Use wild cards.** Enables you to use wild card characters in your search. For example, use an asterisk wildcard (*) to represent a string of characters, or a question mark wild card (?) to represent one character only. ➤ **Match from start.** Search for monitors/monitor categories that match the search text from the start. ➤ **Match exactly.** Search for monitors/monitor categories that exactly match the search text. ➤ **Match anywhere.** Search for monitors/monitor categories that contain the search text somewhere in the name.
Recently Used Monitors	Displays the five most recently selected monitors. Click a link to create a new monitor for the selected monitor type. **Note:** The displayed monitors may change as more selections are made.

UI Element	Description
Available Monitors	Displays the list of available monitors and categories. Select a monitor to deploy from the list of available monitors or by category. To select by category, click the arrow to the right of the **Category** heading, and select a monitor category from the list detailed below. You can change the alphabetical order (ascending or descending) of the listed monitors or categories, by clicking the arrow in the header of the **Monitor** or **Category** column.
Category	You can add a monitor by selecting one of the following categories, and clicking a monitor in that category: ➤ All (default) ➤ Application ➤ Database ➤ Generic ➤ Integration ➤ Media ➤ Network ➤ Server ➤ Virtualization and Cloud ➤ Web Transaction

Common Monitor Settings

The common monitor settings enable you to configure settings for a new monitor.

To access	Select the **Monitors** context. ➤ For new monitors: In the monitor tree, right-click a group, select **New** > **Monitor**, and select a monitor from the New Monitor dialog box. ➤ For existing monitors: In the monitor tree, expand the group folder that contains the monitor, and select the monitor. In the right pane, click the **Properties** tab.
Relevant tasks	"How to Deploy a Monitor" on page 414
See also	"Monitor Tree" on page 81

User interface elements are described below:

UI Element	Description
<Setting panes>	The following setting panes in the monitor Properties tab are common to all monitors. For details on the settings for a specific SiteScope monitor, see the user interface page for the monitor type. ➤ "General Settings" on page 449 ➤ "Monitor Run Settings" on page 451 ➤ "Dependencies" on page 454 ➤ "Threshold Settings" on page 457 ➤ "HP Integration Settings" on page 466 ➤ "Enable/Disable Monitor" on page 479 ➤ "Enable/Disable Associated Alerts" on page 482 ➤ "Search/Filter Tags" on page 484 ➤ "Baseline Settings" on page 485 **Note:** The Link Monitor to CI settings pane was removed in SiteScope 11.00 and the functionality was replaced by the report custom topology feature in the HP Integration Settings pane.

UI Element	Description
Verify & Save	Verifies the correctness of the monitor configuration locally and on the remote server to be monitored, before saving the settings. If SiteScope fails to connect to the remote server, or if there is an invalid property in the configuration settings, verification fails and an error message is displayed. **Tip:** Performance is not as fast if you use **Verify & Save** instead of **Save**, because SiteScope needs to establish a connection to the remote server to verify the settings. For bulk operations such as Publish Template Changes and Global Search and Replace, we recommend using the **Save** option only
Save	Performs a local verification of the configuration settings, and saves the settings (without verifying the correctness of the monitor configuration on the remote server). **Tip:** Performance is faster if you use **Save** instead of **Verify & Save**, because SiteScope does not need to establish a connection to the remote server to verify the settings. For bulk operations such as Publish Template Changes and Global Search and Replace, we recommend using the **Save** option only.

General Settings

The General Settings pane enables you to create a name and description for the monitor instance.

To access	Select the **Monitors** context. In the monitor tree, expand the group folder that contains the monitor, and select the monitor. In the right pane, click the **Properties** tab, and select **General Settings**.
Important information	➤ HTML code entered in the monitor description fields is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. ➤ For buttons common to all panes, see "Common Monitor Settings" on page 447.
Relevant tasks	"How to Deploy a Monitor" on page 414

User interface elements are described below:

UI Element	Description
Name	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 value:** SiteScope creates a default name based on the host, system, and/or URL being monitored or the default name defined for the monitor type.

UI Element	Description
Monitor description	Additional information to describe a monitor. This can include the most common HTML tags for text styling, such as , <HR>, and <B>. The description is displayed only when viewing or editing the monitor's properties in the SiteScope Dashboard. You can also include HTML tags to enable you to access URLs from the SiteScope Dashboard. To add a hyperlink, enter the URL. For example, My Link. The URL is displayed in the **Description** field for the selected monitor in the SiteScope Dashboard. **Note:** This field does not support JavaScript/iframes/frames or other advanced features. HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. The following is prohibited HTML content: ➤ Tags: **script**, **object**, **param**, **frame**, **iframe**. ➤ Any tag that contains an attribute starting with **on** is declined. For example, onhover. ➤ Any attribute with **javascript** as its value.

UI Element	Description
Report Description	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. **Note:** HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. The following is prohibited HTML content: ➤ Tags: **script**, **object**, **param**, **frame**, **iframe**. ➤ Any tag that contains an attribute starting with **on** is declined. For example, onhover. ➤ Any attribute with **javascript** as its value.

Monitor Run Settings

The Monitor Run Settings pane enables you to configure settings for the monitor run.

To access	Select the **Monitors** context. In the monitor tree, expand the group folder that contains the monitor, and select the monitor. In the right pane, click the **Properties** tab, and select **Monitor Run Settings**.
Important information	For buttons common to all panes, see "Common Monitor Settings" on page 447.
Relevant tasks	"How to Deploy a Monitor" on page 414
See also	"Schedule Preferences Overview" on page 836

User interface elements are described below:

UI Element	Description
Frequency	How often SiteScope attempts to run the action defined for the monitor instance. Each monitor run updates the status of the monitor. Use the drop-down list to specify increments of seconds, minutes, hours, or days. **Default value:** 10 minutes **Minimum value:** 15 seconds **Note:** When configuring this setting in a template, the variable value can only be in time units of seconds.
Error frequency	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 monitor run frequency affects the number of alerts generated by the monitor. ➤ When configuring this setting in a template, the variable value can only be in time units of seconds.

UI Element	Description
Verify error	Automatically runs the monitor again if it detects an error. It runs the monitor immediately after the regular run returned an error to make sure that the first error was not a false alert. If the error is returned again, it is reported as a result of the monitor run, and the next run takes place according to the monitor schedule. To change monitor scheduling while the monitor is in error status, see the **Error frequency** setting. This is a preferred and recommended setting over **Verify error**, especially for large SiteScope environments. 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. **Tip:** We recommend using this option in small monitoring environments only. Significant monitoring delays may result if multiple monitors are rescheduled to verify errors at the same time.
Monitor schedule	Range schedule if you want the monitor to run only on certain days or on a fixed schedule. The range schedules created in **Schedule Preferences** appear in the drop-down list. For more information about creating monitor schedules, see "Schedule Preferences Overview" on page 836. **Default value:** every day, all day **Note:** If you select a threshold schedule in the Threshold Settings, at least one threshold schedule must coincide with the monitor run schedule (at least one minute of the monitor run schedule must be covered by one of the threshold schedules).
Show run results on update	Whenever a change is made to a monitor's configuration settings, the monitor is run. Displays 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.

Dependencies

The Dependencies pane enables you to create a dependency relationship that enables you to make the running of this monitor dependent on the status of another monitor.

To access	Select the **Monitors** context. In the monitor tree, expand the group folder that contains the monitor, and select the monitor. In the right pane, click the **Properties** tab, and select **Dependencies**.
Important information	For buttons common to all panes, see "Common Monitor Settings" on page 447.
Relevant tasks	"How to Deploy a Monitor" on page 414
See also	"Monitoring Group Dependencies" on page 397

User interface elements are described below:

UI Element	Description
Depends on	Click **Depends on**  to open the Select Depends On Monitor dialog box, and select the monitor on which you want to make the running of this monitor dependent. For details on the Select Depends On Monitor dialog box, see "Select Depends On Monitor Dialog Box" on page 487. 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 value**: No dependency is set for a monitor instance.

UI 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** box reports the condition selected in this box. **Example:** Select Good and this monitor is enabled only when the monitor selected in the **Depends on** box reports a status of Good. The current monitor is automatically disabled if the monitor selected in the **Depends on** box reports a category or condition other than Good. You can also enable dependent monitors specifically for when a monitor detects an error. **Default value:** Good

Threshold Settings

Use to set conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system during a specified period of time.

Status threshold criteria for each monitor instance can be set for the **Error if**, **Warning if**, and **Good if** status conditions. You can also set monitor thresholds using a baseline to provide a comparison for establishing acceptable or expected threshold ranges. For details, see "Setting Status Thresholds Using a Baseline" on page 405.

To access	Select the **Monitors** context. In the monitor tree, expand the group folder that contains the monitor, and select the monitor. In the right pane, click the **Properties** tab, and select **Threshold Settings**.
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. ➤ When setting a baseline threshold, you can only change certain threshold conditions during the baseline calculation and after the baseline is activated. For details on the threshold changes that are allowed, see "Changing Threshold Settings" on page 465. ➤ When working with Global Search and Replace, if you select to replace threshold settings, the **Override Category** option appears. When selected, all the threshold settings for the selected monitor instances are overridden with the settings you entered for the replace operation. If this option is cleared and you selected to replace threshold settings, the settings you entered are added to the existing threshold settings for the monitor instances. ➤ For buttons common to all panes, see "Common Monitor Settings" on page 447.

Relevant tasks	➤ "How to Deploy a Monitor" on page 414 ➤ "How to Set Monitor Thresholds Using a Baseline" on page 418
See also	➤ "Setting Status Thresholds" on page 400 ➤ "Setting Status Thresholds Using a Baseline" on page 405

User interface elements are described below:

UI Element	Description
	**New.** Creates additional thresholds that determine the **Error**/**Warning**/**Good** status. For each threshold, select the measurement and operator, and enter a value for the measurement. By default, two thresholds are displayed for the **Error** status when you first configure the monitor, and one threshold for the **Warning** and **Good** status.
	**Delete.** Deletes the selected threshold.

UI Element	Description
If unavailable	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 "SiteScope Alerts Overview" on page 1417.
Default status	Monitor status (**Good**, **Warning**, or **Error**) if the threshold criteria for the monitor instance are not met. **Default value:** Good

UI Element	Description
On internal error	Monitor status assignment if a configuration or internal error occurs: ➤ **Set monitor status according to Thresholds.** The monitor's status is set according to its current thresholds if a configuration or internal error occurs (default setting). It is unreliable to rely on the threshold since there is no way of knowing at what point the error occurred (and whether the threshold is based on old data, updated data, or both). For example, a monitor may remain in its current status even though the monitor did not run; change status if thresholds were defined that were not applicable; or trigger false alerts as if a remote was not available, when in fact, the remote was not contacted. ➤ **Set monitor status to Error.** The monitor's status is set to Error if a configuration or internal error occurs without thresholds being checked. ➤ **Set monitor status to Warning.** The monitor's status is set to Warning if a configuration or internal error occurs without thresholds being checked. ➤ **Set monitor status to Good.** The monitor's status is set to Good if a configuration or internal error occurs without thresholds being checked. ➤ **Treat monitor as unavailable.** The monitor is treated as being Unavailable if a configuration or internal error occurs without thresholds being checked.
Add Default Thresholds	Adds default threshold settings to the monitor instance, for the applicable status categories. Default thresholds are indicated by the **(default)** label. Default thresholds are editable only after selecting a condition from the **Condition** field (the default condition can be selected). After any criteria of the default threshold is changed, the **(default)** label is removed.
Remove Default Thresholds	Deletes the default threshold settings (those indicated by the **(default)** label) from the monitor instance. Default settings that were added and were subsequently modified, are not removed.

UI Element	Description
Threshold Preview	Opens the Threshold Preview dialog box that displays a preview of thresholds for static counters and for regular expression patterns translated to actual current counters. Patterns enable the monitor to automatically configure itself with counters and thresholds on the relevant dynamic environment components (currently available for VMware Host monitors). The table also displays an **Indicator State and Severity** value for each current counter translated from a pattern (this value is not available for patterns in Threshold Settings). For more details on dynamic monitors, see "VMware Host Monitors Overview" in *Monitor Reference*. **Example:** The pattern /.*/VirtualMachine/.*/cpu/usage.average\[\]/ displays the average CPU usage threshold condition for each VM currently being monitored.
Error if	Conditions for the monitor instance to report an **Error** status.
Condition	Measurement parameter for determining the status of this monitor instance. The list of measurements is dynamically updated based on the type of monitor you are configuring. **Default value:** Default measurements exist for many monitor types and differ per monitor type. For many default measurements, there are corresponding defaults for the operator and value boxes that are not editable.

UI Element	Description
Operator	Measurement operator for determining the status of this monitor instance. The following operators are available: ➤ >= 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 **Note:** To indicate data volatility (where current monitor readings significantly deviate from previous runs), set status thresholds using a baseline. For details, see "Setting Status Thresholds Using a Baseline" on page 405.
Value	Value applicable to the measurement parameter. **Note:** ➤ If a monitor has an activated baseline, its measurement values are non-editable and the **Percentiles Table** button is displayed. You can change baseline threshold values by clicking the button and changing the current percentile value from the Percentiles Table. For user interface details, see "Percentile Range Mapping Table" on page 491. ➤ You cannot change the measurement value, operator or schedule for a baseline threshold condition.

UI Element	Description
Schedule	Range schedule to determine the status of this monitor instance if you want to define when to check the monitor run result against the threshold. This is useful, for example, if you want to check the monitor run result against the threshold only on certain days or during peak hours. The range schedules created in **Schedule Preferences** appear in the drop-down list. For more information about creating monitor schedules, see "Schedule Preferences Overview" on page 836. **Default value:** every day, all day **Note:** When selecting threshold schedules, at least one threshold schedule must coincide with the **Monitor schedule** in the Monitor Run Settings (at least one minute of the monitor run schedule must be covered by one of the threshold schedules).

UI Element	Description
Indicator State and Severity	State of the indicator (for example, Bottlenecked), and the severity corresponding to the indicator state (for example, Critical). Every indicator can have several states. For example, when measuring CPU Load, the indicator state might be Bottlenecked or Busy, whereas when measuring Memory Load, the indicator state might be Paging or Starving for Memory. Indicator state and severity level are mapped to metric status according to the closest available severity that exists in the states for the indicator associated with the metric. The indicator state and severity values are updated when a different indicator mapping is selected in the HP Integration Settings pane. For more information on indicator mappings, see "SiteScope Metrics Assigned to Indicators" on page 403. **Note:** ➤ SiteScope must be connected to BSM 9.00 or later for the **Indicator State and Severity** column to be displayed. ➤ Indicator state and severity values are not displayed in SiteScope reports. ➤ If the **Indicator State and Severity** box is empty, the metric is not colored in Service Health, except for **always (default)** which is automatically assigned. ➤ To display the **Indicator State and Severity** value for each current counter for a dynamic monitor (these are the actual counters translated from a regular expression pattern), click the **Threshold Preview** button. The indicator state and severity value is displayed for each actual counter in the Threshold Preview dialog box. ➤ The association between the indicator state and severity cannot be changed on the local SiteScope server.

UI Element	Description
Warning if	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.
Good if	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.

Changing Threshold Settings

You can make changes to threshold conditions according to the baseline status of the monitor instance.

Monitor Baseline Status	Change Threshold Condition	Add/Delete Threshold Condition
Not baselined	You can change any condition of any threshold.	Allowed
In calculating/ activating process	You can only change the measurement value for static thresholds. For example, Error if CPU >= 70 every day, all day, you can only change the value 70 to another value.	Not allowed
Baselined	➤ You can change any condition for static thresholds. ➤ You can change the percentile value only for baseline thresholds.	Allowed for static thresholds only

HP Integration Settings

The HP Integration Settings pane enables you to control what data a monitor forwards to the applications integrated with SiteScope.

To access	Select the **Monitors** context. In the monitor tree, expand the group folder that contains the monitor, and select the monitor. In the right pane, click the **Properties** tab, and select **HP Integration Settings**.
Important information	➤ For buttons common to all panes, see "Common Monitor Settings" on page 447. ➤ The HP Integration Settings panel is displayed only when SiteScope is integrated with BSM, or when SiteScope is integrated with HP Operations Manager (HPOM) and event or metrics integration is enabled. ➤ The custom topology is available only if SiteScope is connected to BSM version 9.00 or later. ➤ The indicator settings are available only if SiteScope is connected to BSM version 9.00 or later or to HPOM. ➤ The HP Operations Manager integration settings are available only if an OM integration has been configured and SiteScope is connected to HPOM. For details on configuring the OM Integration, see "HP Operations Manager Integration Dialog Box" on page 776.
Relevant tasks	➤ "How to Deploy a Monitor" on page 414 ➤ "How to Configure the Integration Between SiteScope and BSM" on page 288
See also	"Integration Preferences" on page 741

BSM Integration Data and Topology Settings

This section enables you to select BSM logging options and topology reporting settings for the monitor instance.

Important information	➤ The BSM logging options are available only if BSM integration is enabled. ➤ The **Enable reporting changes in status** option was removed due to the introduction of event management in BSM. This option can be enable for backward compatibility by changing the property **_allowToSendOnlyMonitorStatusToBSM9** to **=true** in the **<SiteScope root directory>\groups\master.config** file. ➤ BSM logging selection should be based on how much data is relevant to report to BSM for this monitor and how much space the BSM database has for this data. ➤ For troubleshooting problems involving topology reporting, see "Business Service Management Topology Issues" in *Integration with Business Service Management and Operations Manager Best Practices* in the SiteScope Help.
Relevant tasks	➤ "How to Deploy a Monitor" on page 414 ➤ "How to Configure the Integration Between SiteScope and BSM" on page 288 ➤ "How to Configure Topology Reporting" on page 298
See also	"Integration Preferences" on page 741

Relevant tasks	➤ "How to Deploy a Monitor" on page 414 ➤ "How to Configure the Integration Between SiteScope and BSM" on page 288 ➤ "How to Configure Topology Reporting" on page 298
See also	"Integration Preferences" on page 741

User interface elements are described below:

UI Element	Description
BSM Logging Options	
Disable reporting metrics to BSM	Prevents the status information or metrics for this monitor being transferred to BSM or temporarily disables reporting this monitor to BSM.
Enable reporting monitor status and metrics	Sends all monitor data to BSM for each time that the monitor runs. This option enables the largest data transfer load. **Default value:** Selected
Enable reporting monitor status (no metrics)	Sends 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. **Note:** This option is supported only for backward compatibility with legacy SLM, and not for Service Health.
Enable reporting monitor status and metrics with thresholds	Sends monitor category (**error**, **warning**, **good**), status string, as well as performance counter data for only those metrics counters that have configured thresholds (for example, Error If, Warning If, Good if). The data is sent for each time that the monitor is run.

UI Element	Description
Topology Settings	
Report monitor and related CI topology	SiteScope reports monitor and related CI topology data to BSM's RTSM (Run-time Service Model). The data that SiteScope forwards depends on the monitor type. This option enables SiteScope to: ➤ Discover topologies and forward specific CI data for the monitors that monitor applications from among a group of supported environments. For details and a list of these supported environments, see "Reporting Discovered Topologies to BSM" on page 282. ➤ Report Node CI data for those monitors that monitor hosts (SiteScope sends Computer CI type for each monitored host). If this option is selected, the monitor creates a topology that includes the host as a CI in BSM's RTSM. ➤ Report CI data based on the user-defined CI type and key attribute values. If cleared, the monitor and related CI topology data is not reported to BSM (and the Indicator Settings). For details on how SiteScope reports data to the RTSM, see "Integrating SiteScope Data with BSM's Configuration Items" on page 273. **Note:** If SiteScope is connected to BSM (and you have an Event Management Foundation license), and sending events is enabled, hosts are reported to BSM through Operations Management. **Default value**: ➤ Selected for monitors of supported environments and monitors that have a CI type defined by default. ➤ Cleared for monitors that do not have a topology defined by default. For a list of these monitors, see "Monitors Not Reporting Topology Data By Default" on page 302.

UI Element	Description
CI type	The monitor's topology that is used for reporting data to BSM's RTSM. You can link between this monitor instance and any existing, logical configuration item type (CIT) in BSM's RTSM. This link or relationship enables the monitor to pass KPI status to the CI to which it is linked. The CI type indicates the following: ➤ **Default (<CI type>).** The default CI type for the monitor (for most monitors, the default CI type is Computer). For a list of monitors where the default CI type is not Computer, see "Supported Environments" on page 283. CI types include BusinessApplication, BusinessService, DB2, InfrastructureService, JBoss AS, Node, Oracle, Oracle iAS, SQL Server, Sybase, Unix, WebLogic AS, WebSphere AS, and Windows. ➤ **Default (Multiple).** The monitor has multiple CIs (this is where the CI type is per metric). The CI type for these monitors is fixed and cannot be modified. For a list of these monitors, see "Monitors Reporting CI Per Metric" on page 303. ➤ **None.** The monitor instance is not linked to a CI type. For a list of these monitors, see "Monitors Not Reporting Topology Data By Default" on page 302. You can select a CI type from an RTSM view to link to this monitor instance. For details on selecting and working with views, see "Working with the CI Selector" in the *Modeling Guide* in the HP Business Service Management Documentation Library. **Note:** ➤ This setting is active only when **Report monitor and related CI topology** is selected. ➤ After a CI type is selected, the Indicator Settings table is filtered to show mappings that exist for the selected CI type only.

UI Element	Description
<CI type key attributes>	CI type key attributes are displayed according to the CI type selected for the monitor instance. Enter the key attribute values for the selected CI type: ➤ **Server.** Container CI for the selected CI. This attribute is required for DB2, JBoss AS, Oracle, Oracle iAS, SQL Server, Sybase, WebLogic AS, WebSphere AS, and Windows CI types. ➤ **Name.** ➤ Name of the CI (for BusinessApplication, BusinessService, Computer, DB2, InfrastructureService, JBoss AS, Oracle, Oracle iAS, SQL Server, Sybase, WebLogic AS, and WebSphere AS CI types). ➤ **Organization Type.** Identifier used to differentiate levels within an organization. This attribute is required for BusinessApplication, BusinessService, and InfrastructureService CI types. ➤ **Organization Name.** Name of the organization. This attribute is required for BusinessApplication, BusinessService, and InfrastructureService CI types. **Note:** ➤ This setting is active only when **Report monitor and related CI topology** is selected. ➤ CI key attributes are not available for monitors where the CI type is per metric. For a list of these monitors, see "Monitors Reporting CI Per Metric" on page 303.

Indicator Settings

This section displays the metrics for the SiteScope monitor type and the health indicators (HIs) and event type indicators (ETIs) to which the metric is assigned. Indicators provide a more detailed view of the health of a configuration item (CI) when the monitor's topology is reported to BSM's RTSM. The Indicator Settings table is filtered to show mappings for the monitor instances that exist for the selected CI type only.

Important information	➤ Indicator Settings are available only if HP Operations Manager event integration or BSM integration is enabled, and: ➤ The **Report monitor and related CI topology** setting is selected in BSM integration Data and Topology Settings section. ➤ The monitor has default metric-to-indicator mappings. For a list of monitors that do not have default indicator mappings, see "Monitors Not Reporting Topology Data By Default" on page 302. ➤ Indicator settings cannot be added or deleted where the CI type is per metric (Default (Multiple)). For a list of these monitors, see "Monitors Reporting CI Per Metric" on page 303. ➤ The indicator assignments table in SiteScope might contain assignments that do not exist in the Indicator Assignments repository in BSM. This is because mappings that are incorrectly defined in BSM are not validated when they are downloaded to SiteScope (whereas they are validated, and therefore, not displayed in BSM). ➤ Only advanced users with a thorough knowledge of CIs and indicators should attempt to edit any of the indicator mappings or to add mappings to metrics. ➤ If any of the settings in the indicator mapping table are modified by a user, a note to indicate this is displayed below the table.
Relevant tasks	➤ "How to Deploy a Monitor" on page 414 ➤ "How to Configure Topology Reporting" on page 298
See also	"Assigning SiteScope Metrics to Indicators" on page 279

User interface elements are described below:

	**New.** Enables you to add a metric-to-indicator mapping to a monitor instance based on the monitor type.
	**Delete.** Deletes the selected metric-to-indicator mapping.
	**Reset to Default.** Resets the metric-to-indicator mapping for the monitor type to the default mappings included in your current version of SiteScope. Indicators mappings are stored in a central repository in System Availability Management (SAM) in BSM. SiteScope checks every 5 minutes to see if the mappings in SAM have changed, and if they have, downloads the latest mappings. If indicator mappings on a local SiteScope server have been modified, these mappings are not overridden by the centralized mappings when the topology is next reported to BSM. For details on modifying the centralized mappings, see "Indicator Assignment Settings" in *Using System Availability Management* in the HP Business Service Management Documentation Library.
	**Move Down.** Enables you to change the sort order of the indicator mappings by moving the selected indicator mapping down the list. If the mapping order is changed locally, the local mapping order is not overridden when mapping changes are downloaded from the Indicator repository in SAM Admin.
	**Move Up.** Enables you to change the sort order of the indicator mappings by moving the selected indicator mapping up the list. If the mapping order is changed locally, the local mapping order is not overridden when mapping changes are downloaded from the Indicator repository in SAM Admin.

Metric Pattern	Displays a regular expression pattern based on the metric name. You can modify an existing mapping or create a new one. Where there is more than one CI type for the same regular expression, they are displayed in different rows. For details on using regular expressions, see "Using Regular Expressions" on page 235.
CI Type	Displays the CI type selected for the monitor instance (the Indicator Settings table is filtered to show mappings that exist for the selected CI type only). **Note:** This field is not editable.
Indicator	Displays the indicator mapping for the metric. In the drop-down list, health indicators are displayed above the divider line, and event type indicators below the line.

HP Operations Manager Integration Settings

This section enables you to configure SiteScope to send events and report metrics to the HP Operations agent. The agent is required for sending events to HPOM and BSM's Operations Management, and for reporting metrics to HP Performance Manager (a reporting component of HPOM) and Operations Management. It also enables you to select the event preference mapping that is used for sending events for the monitor instance.

Important information	These settings are available only if the HP Operations agent is installed and connected to an HPOM server, and event/metrics integration is enabled in the HP Operations Manager Integration dialog box.
Relevant tasks	➤ "How to Deploy a Monitor" on page 414 ➤ "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326 ➤ "How to Enable SiteScope to Report Metrics to the HP Operations Agent" on page 349 ➤ "How to Configure Common Event Mappings" on page 822
See also	➤ "Integration Preferences" on page 741 ➤ "Common Event Mappings" on page 819

User interface elements are described below:

Report metrics to HP Operations agent	Enables SiteScope to report metrics for the monitor instance to the HP Operations agent, from which HPOM and Operations Management (in BSM) can collect the data. **Note:** Monitor metrics are sent to the agent only if metrics integration is enabled in the HP Operations Manager Integration dialog box. For user interface details, see "HP Operations Manager Metrics Integration" on page 782. **Default value**: Selected if metrics integration is enabled (otherwise this setting is not available).
Send events	Enables sending events to HPOM or Operations Management (in BSM) when there is a change of a counter/metric status (**Good**/**Warning**/**Error**/**Unavailable**) for the monitor instance. Status change is only applicable on counters or metrics that are configured in the monitor's Threshold Setting. **Note:** This setting is available only if the HP Operations agent is installed and connected to an HPOM or BSM server, and event integration is enabled in the HP Operations Manager Integration dialog box. For user interface details, see "HP Operations Manager Integration Main Settings" on page 777. **Default value**: Selected if event integration is enabled (otherwise this setting is not available).

Event mapping	The event mapping template used for sending events for the monitor instance. The template contains mappings between SiteScope runtime data and the attribute values that are used for sending events. Select the desired event mapping template, or use the default mapping. Click **New** or **Edit** to open the Common Event Mappings dialog box and configure a new event preference or modify an existing one. For user interface details, see "New/Edit Event Mapping Dialog Box" on page 826. **Note:** ➤ This setting is available only if the HP Operations agent is installed and connected to an HPOM or BSM server, and event integration is enabled in the HP Operations Manager Integration dialog box. For user interface details, see "HP Operations Manager Integration Main Settings" on page 777. ➤ When editing an event mapping from here, it changes the event pattern for all monitors using this template. We recommend creating a new event mapping if you want a specific monitor to report different attributes.
Manually send first event	When creating a new monitor in a SiteScope connected to BSM, it is possible that the first event is triggered before the topology is reported to BSM, and the event is lost from the Service Health perspective (it is still shown in the Operations Management Event Browser). Select this option to avoid waiting for the next event to be sent. The event is resent during the next monitor run, regardless of the monitor's metrics reaching their status change conditions. **Default value**: Not selected **Note:** ➤ This option is automatically disabled after the monitor run. ➤ You can configure this setting globally using Global Search and Replace.

BSM Service Health Preferences

This section enables you to configure the preference for influencing BSM's Service Health when both SiteScope events and metrics are reported to BSM.

Important information	This setting is available only when: ➤ Both BSM and HP Operations Manager integrations are active, and are connected to the same BSM server (the BSM server is used instead of the HPOM server). ➤ The following settings are selected in the monitor's HP Integration Settings: ➤ In BSM Integration Data and Topology Settings Settings: **Enable reporting monitor status and metrics** or **Enable reporting monitor status and metrics with thresholds**, and ➤ In HP Operations Manager Integration Settings: **Send events**. **Note:** ➤ If only **Send events** is selected, the **BSM Service Health affected by** preference is set to **Events**. ➤ If only **Report monitor and related CI topology** is selected, the **BSM Service Health affected by** preference is set to **Metrics**. ➤ If both are selected, **Metrics** is the default preference.
Relevant tasks	➤ "How to Deploy a Monitor" on page 414 ➤ "How to Configure Topology Reporting" on page 298 ➤ "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326

User interface elements are described below:

BSM Service Health affected by	Select the preference (events or metrics) for influencing BSM's Service Health when both SiteScope events and metrics are reported to Service Health (since indicators for SiteScope events and metrics both affect CIs). ➤ **Metrics.** If selected, each SiteScope measurement affects CIs in BSM (status change events reported by SiteScope do not have any influence on CIs in Service Health). ➤ **Events** If selected, only status change events affect CIs in BSM's Service Health (SAM reports for the monitored CIs are still based on metrics). For more information on choosing the preference to use, see "Integrating SiteScope with Business Service Management Applications" in *Best Practices for the SiteScope-Business Service Management/Operations Manager Integration* in the SiteScope Help. **Default value**: Metrics **Note:** You can also configure a global default preference (events or metrics) for all new monitors created when configuring the HP Operations Manager integration. For details, see **Prefer events over metrics in BSM Service Health (global preference)** in "HP Operations Manager Integration Main Settings" on page 777.

Enable/Disable Monitor

The Enable/Disable Monitor pane enables you to set the status (enabled/disabled) for the selected monitor.

To access	Select the **Monitors** context. In the monitor tree, expand the group folder that contains the monitor, and select the monitor. In the right pane, click the **Properties** tab, and select **Enable/Disable Monitor**.
Important information	➤ HTML code entered in the monitor description fields is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. ➤ The Monitor Downtime table is displayed only when SiteScope is connected to BSM if the selected monitor is affected by a CI currently in downtime. For details, see "CI Downtime" on page 285. ➤ For buttons common to all panes, see "Common Monitor Settings" on page 447.
Relevant tasks	"How to Deploy a Monitor" on page 414
See also	"Enable/Disable Monitors in Group Dialog Box" on page 1321

User interface elements are described below:

UI Element	Description
Enable monitor	Enables the monitor if the monitor was previously disabled. **Default value:** Selected
Disable monitor	Disables the monitor. 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 run. SiteScope records a monitor data log entry for the monitor when it was scheduled to be run but reports the monitor status as disabled in the place of metrics data.
Disable monitor for the next <time period>	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 from <time> to <time>	Temporarily disables the monitor for a time period in the future. The time period can span more than one day. Enter or select the start time and end time for the disable period using the format: hh:mm:ss mm/dd/yyyy.
Disable description	Optional descriptive text that 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** option.

UI Element	Description
Monitor Downtime Table (This table is displayed only when SiteScope is connected to BSM if the selected monitor is affected by a CI currently in downtime. For details, see "CI Downtime" on page 285.)	
Downtime Name	The name of the downtime as configured in the BSM Downtime wizard.
Downtime Description	A description of the downtime if entered in the BSM Downtime wizard.
Current Occurrence End Date	Date and time that the current downtime occurrence is scheduled to end.

Enable/Disable Associated Alerts

The Enable/Disable Associated Alerts pane enables you to set the status (enabled/disabled) for associated alerts.

To access	Select the **Monitors** context. In the monitor tree, expand the group folder that contains the monitor, and select the monitor. In the right pane, click the **Properties** tab, and select **Enable/Disable Associated Alerts**.
Important information	➤ HTML code entered in the monitor description fields is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. ➤ The Associated Alerts Downtime table is displayed only when SiteScope is connected to BSM if the monitor is affected by a CI that is currently in downtime, and the downtime applies to associated alerts of the monitor. For details, see "CI Downtime" on page 285. ➤ For buttons common to all panes, see "Common Monitor Settings" on page 447.
Relevant tasks	➤ "How to Deploy a Monitor" on page 414 ➤ "How to Configure an Alert" on page 1443
See also	"SiteScope Alerts Overview" on page 1417

User interface elements are described below:

UI Element	Description
Enable all associated alerts	Enable the alerts if the alerts associated with this monitor were previously disabled. **Default value:** Selected
Disable all associated alerts for the next <time period>	Time period that the associated alerts should remain disabled. Select **Seconds**, **Minutes**, **Hours**, or **Days** to define the disable time period as applicable.

UI Element	Description
Disable all associated alerts on a one time schedule from <time> to <time>	Temporarily disables the associated alerts for a time period in the future. The time period can span more than one day. Enter the start time and end time for the disable period using the format: hh:mm:ss mm/dd/yyyy.
Disable description	Optional descriptive text.
Associated Alerts Downtime Table (This table is displayed only when SiteScope is connected to BSM if the monitor is affected by a CI that is currently in downtime, and the downtime applies to associated alerts of the monitor. For details, see "CI Downtime" on page 285.)	
Downtime Name	The name of the downtime as configured in the BSM Downtime wizard.
Downtime Description	A description of the downtime if entered in the BSM Downtime wizard.
Current Occurrence End Date	Date and time that the current downtime occurrence is scheduled to end.

Search/Filter Tags

The Search/Filter Tags pane enables you to add a new search/filter tag, and assign the tag to objects in the context tree and preference profiles. Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required.

To access	Select the **Monitors** context. In the monitor tree, expand the group folder that contains the monitor, and select the monitor. In the right pane, click the **Properties** tab, and select **Search/Filter Tags**.
Important information	➤ You can edit existing tags in the Preferences context (**Preferences** > **Search/Filter Tags**). For details on this topic, see "Search/Filter Tags Overview" on page 904. ➤ For buttons common to all panes, see "Common Monitor Settings" on page 447.
Relevant tasks	➤ "How to Deploy a Monitor" on page 414 ➤ "How to Create and Define a New Search/Filter Tag" on page 119
See also	"Working with Search/Filter Tags" on page 118

User interface elements are described below:

UI Element	Description
<Tag name and values>	Displays the tag names and tag values if tags have been created. Select the tags or tag values that you want to assign to the object. If no tags have been created for the SiteScope, this section appears but is empty.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

Baseline Settings

The Baseline Settings pane displays the baseline status for the selected monitor.

To access	Select the **Monitors** context. In the monitor tree, expand the group folder that contains the monitor, and select the monitor. In the right pane, click the **Properties** tab, and select **Baseline Settings**.
Important information	➤ For buttons common to all panes, see "Common Monitor Settings" on page 447. ➤ Baseline Settings are not available for monitors that use the dynamic monitoring mechanism to update thresholds settings.
Relevant tasks	➤ "How to Deploy a Monitor" on page 414 ➤ "How to Set Monitor Thresholds Using a Baseline" on page 418
See also	"Setting Status Thresholds Using a Baseline" on page 405

User interface elements are described below:

UI Element	Description
Baseline status	The monitor's baseline status. The following statuses are available: ➤ **Monitor not selected for baselining.** The monitor has not been selected for baselining. ➤ **Calculating baseline.** SiteScope is in the process of calculating the baseline. ➤ **Calculation failed.** SiteScope was unable to calculate a baseline. ➤ **Calculated, not activated.** A baseline was calculated for the monitor, but it has not yet been activated. ➤ **Activating baseline.** SiteScope is in the process of activating the baseline. ➤ **Activation failed.** SiteScope was unable to activate the baseline. ➤ **Baseline activated.** The baseline has been activated for the monitor. The **Baseline mode** check box is selected if the baseline status is anything other than **Monitor not selected for baselining**. For details on using the baseline threshold, see "Setting Status Thresholds Using a Baseline" on page 405.
Remove Baseline	Removes the baseline threshold. The baseline thresholds are removed and the static threshold value is used to create a threshold. You must remove the baseline before you can calculate the baseline after a baseline has been calculated (even if the calculation failed). For details on this topic, see "Setting Status Thresholds Using a Baseline" on page 405.

Select Depends On Monitor Dialog Box

This dialog box enables you to make the running of this monitor or monitor group dependent on the status of another monitor.

To access	Select the **Monitors** context. In the monitor tree, select a monitor, and click the **Properties** tab. Expand the **Dependencies** tab, and click **Depends on**  . Select the monitor on which to you want to create a dependency.
Relevant tasks	"How to Deploy a Monitor" on page 414
See also	➤ "Monitoring Group Dependencies" on page 397 ➤ "Monitor Tree" on page 81

User interface elements are described below:

UI Element	Description
	Represents an individual SiteScope server.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors). If a group alert has been set up for the monitor group or subgroup, the alert symbol is displayed next to the group icon.
	Represents a SiteScope monitor (enabled/disabled). If an alert has been set up for the monitor, the alert symbol is displayed next to the monitor icon.
	Represents the collection of available health monitors that are deployed to check proper functioning of SiteScope monitors. **Parent:** SiteScope.

Select Template Dialog Box

This dialog box enables you to select the templates you want to deploy to the monitor group.

To access	Select the **Monitors** context. In the monitor tree, right-click the group into which you want to deploy a template, and select **Deploy Template** or **Deploy Template Using CSV**.
Important information	➤ Templates that do not contain any child objects (subgroups, monitors, variables, or a remote server) are not displayed in the template tree. ➤ Solution templates are not displayed in the Select Template dialog box and can be deployed from the Template context only. For details, see "How to Deploy a SiteScope Solution Template" on page 1088.
Relevant tasks	"How to Configure a SiteScope Monitoring Solution Using a Template" on page 964
See also	➤ "Updating Template Deployments" on page 1032 ➤ "SiteScope Solution Templates" on page 1083 ➤ "Monitor Tree" on page 81 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
	Represents the SiteScope root group.
	Represents a template container. A template container is used to organize configuration deployment templates. Expand to display the templates.
	Represents a template configuration for deploying SiteScope objects. Select the templates that you want to deploy. You can select multiple templates using the CTRL or SHIFT keys.

Copy to Template Tree Dialog Box

This dialog box enables you to copy a SiteScope object (group, monitor, or remote server) and its contents (monitors, alerts, and reports) to a template or template group.

To access	In the monitor or remote server tree, right-click the object you want to copy to a template, and select **Copy to Template**. In the Copy to Template Tree dialog box, select the destination to which to copy the template object.
Important information	➤ You can copy a group and its contents to a template provided the template does not already contain a group. ➤ When copying a server monitor to a template, SiteScope replaces the server name with the $$SERVER_LIST$$ variable. **Tip:** We recommend creating a remote server in the template after copying the monitor to the template, and replacing the $$SERVER_LIST$$ variable with this remote server. ➤ The Web Script Monitor is not supported in template mode.
Relevant tasks	"How to Configure a SiteScope Monitoring Solution Using a Template" on page 964
See also	➤ "Monitor Tree" on page 81 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
	Represents an individual SiteScope server.
	Represents a template container. A template container is used to organize configuration deployment templates. Template containers can hold templates only.

UI Element	Description
	Represents a template configuration for deploying SiteScope objects. You can copy a template group (provided the template does not already contain a group), or a remote server to a template group.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors). You can copy a template group or monitor to a template group. If a group alert has been set up for the monitor group or subgroup, the alert  symbol is displayed next to the group icon.

Percentile Range Mapping Table

This table displays the actual value that is mapped to each percentile range. SiteScope uses the percentile value to define the baseline error and warning thresholds. Use this table to view the actual value that corresponds to the percentile value, and to manually change the percentile value.

To access	Select the **Monitors** context. In the monitor tree, select a monitor with an activated baseline (you can check whether a monitor has an activated baseline by right-clicking a group or monitor, and select **Baselining** > **Status Report**). Expand the monitor's **Threshold Settings**, and click the **Percentiles Table** button.
Important information	➤ This table is available for monitors with an activated baseline only. ➤ You can set the current percentile to a value over 100%. This enables you to raise the threshold level above the level that would have been set, based on the sample measurements collected. For example, if measurements collected for CPU Utilization are between 10%-60%, and you only want to get errors above 80% CPU Utilization, set the percentile value to a percentile that raises the error threshold level to the desired level. In this instance, set the percentile to 134% (60% CPU Utilization * 134% = 80.4% CPU Utilization).
Relevant tasks	"How to Set Monitor Thresholds Using a Baseline" on page 418
See also	➤ "Setting Status Thresholds Using a Baseline" on page 405 ➤ "Threshold Settings" on page 457

User interface elements are described below:

UI Element	Description
Percentiles Range	Percentile range that correlates to the actual value used for defining the baseline error and warning thresholds. You can set the number of percentile ranges displayed in the table from the SiteScope Preferences (**Preferences** > **Infrastructure Preferences** > **Baseline Settings**). **Note:** The left-hand value is exclusive and the right-hand value is inclusive. This means that for a percentile range of 33-100, all values above 33 (but not 33 itself) up to 100 are included in the range. The value 33 falls into the previous range and 100.01 falls into the next range.
Actual Value	The actual value that is mapped to the percentile range.
Current Percentile	Percentile value that correlates to the actual value that is used to define the baseline thresholds.

Calculate Baseline Dialog Box

This dialog box enables you to select the groups, monitors, or both, to include in the baseline calculation, select the time range schedule for collecting baseline data, select and fine-tune the adherence level to determine the extent that monitor measurement sample values have on the threshold values, and calculate the baseline threshold.

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope container, a group, or a monitor, and select **Baselining** > **Calculate**.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit monitors** permissions can use the baseline feature to set monitor thresholds, and only for the monitors that are in the users allowed groups list. Monitors in groups for which the user does not have permissions are not displayed in the dialog box. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ The amount of time required to calculate the baseline thresholds depends on the speed of the SiteScope server and the number of monitors selected for baselining. If SiteScope needs to restart before the calculation process is complete, SiteScope automatically continues the process after the restart. ➤ You should enable the monitors to run for a period that is long enough for SiteScope to accumulate sufficient data to calculate the baseline. This period depends on the **Minimum number of days required for baselining** and **Minimum number of samples required for baselining** settings in Infrastructure Preferences. For details, see "Baseline Settings" on page 735. The baseline can still be calculated and activated even if the monitor has insufficient data, although the calculation is unlikely to be accurate.
Relevant tasks	"How to Set Monitor Thresholds Using a Baseline" on page 418
See also	"Setting Status Thresholds Using a Baseline" on page 405

Select Monitors for Baseline Calculation

User interface elements are described below:

UI Element	Description
<List of available groups and/or monitors>	Groups, monitors, or both, to include in calculating the baseline threshold. The list includes the currently selected container and all of the child containers that are in the users allowed groups list. **Default value:** The current container and all child elements are selected. **Note:** You cannot select a monitor instance if: ➤ Its baseline has already been activated. In such cases, the selection check box is not displayed. ➤ There is another monitor in SiteScope with the same name (the file path, group name, and monitor name are identical). In such cases, **Duplicate name** is displayed next to the monitor name.

Schedule

User interface elements are described below:

UI Element	Description
Schedule Range Name	Schedule ranges used for collecting baseline threshold data. This enables you to restrict to certain days or hours of the week the periods during which monitor data is collected for the baseline calculation. The baseline thresholds that are created are only effective for the same schedule range period. The range schedules displayed are created in **Schedule Preferences**. For more information about creating range schedules, see "Schedule Preferences Overview" on page 836. **Note:** You can select multiple ranges using the CTRL or SHIFT keys. **Default value:** If no schedule range is selected, baseline threshold data is collected all day, every day.

Adherence Level

User interface elements are described below:

Description	Enables you to select the adherence level that determines the extent to which monitor measurement sample values used in calculating the baseline affect the threshold values. The adherence level is based on a percentile value that is applied to all monitor measurements to determine when a measurement is in error or warning. You can also fine-tune the adherence level for individual monitor measurements, and set the Good Boundary. **To access:** In the monitor tree, right-click the SiteScope container, a group, or a monitor, and select **Baselining** > **Calculate**. Expand the **Adherence Level** pane.
Relevant tasks	"How to Set Monitor Thresholds Using a Baseline" on page 418
See also	"Setting the Baseline Adherence Level" on page 409

User interface elements are described below:

UI Element	Description
Low adherence	The further the values used to update the thresholds are from the values calculated by the baseline. Select this option if you are more tolerant to extreme measurement values having an effect on the baseline.
Medium adherence	The values used to update the thresholds are at a mid-range from the values calculated by the baseline (default setting).

UI Element	Description
High adherence	The closer the values used to update the thresholds are to the values calculated by the baseline. Select this option if you are less tolerant to extreme measurement values having an effect on the baseline.
Fine-Tune Adherence Levels/Set Boundary	Opens the Fine-Tune Adherence Levels/Set Boundary dialog box, enabling you to fine-tune the baseline adherence level and define a good boundary for any measurement of any monitor type within the selected context. For user interface details, see "Fine-Tune Adherence Levels/Set Boundary Dialog Box" on page 497.

Fine-Tune Adherence Levels/Set Boundary Dialog Box

This dialog box displays the percentile value used in the baseline calculation at each adherence level and the good boundary (if configured), for each monitor measurement in the selected context. This enables you to fine-tune the baseline adherence level and set good boundaries for any measurement of any monitor type.

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope container, a group, or a monitor, and select **Baselining** > **Calculate**. Expand the **Adherence Level** pane, and click the **Fine-Tune Adherence Levels/Set Boundary** button.
Important information	You can set adherence level percentile values to over 100%. This enables you to raise the threshold level above the level that would have been set, based on the sample measurements collected. For example, if measurements collected for CPU Utilization are between 10%-60%, and you only want to get errors above 80% CPU Utilization, set the **Error Percentiles Low** value to a percentile that raises the error threshold level to the desired level. In this instance, set the percentile to 134% (60% CPU Utilization * 134% = 80.4% CPU Utilization).
Relevant tasks	"How to Set Monitor Thresholds Using a Baseline" on page 418
See also	"Setting Status Thresholds Using a Baseline" on page 405

User interface elements are described below:

UI Element	Description
Reset	**Reset.** Restores the default error and warning threshold adherence level values for the monitor measurement and to remove the Good Boundary.
	**Select All.** Selects all listed monitor measurements.
	**Clear Selection.** Clears the selection.

UI Element	Description
Monitor Name: Measurement Name	For each monitor in the selected context, displays the measurements that are used in the baseline calculation. It also displays one measurement that represents the measurements for all browsable monitors (at the bottom of the list).
Warning Percentiles	Displays the **Low**, **Medium**, and **High** adherence level percentile value that is used to calculate the warning baseline threshold. For more details on this topic, see "Setting the Baseline Adherence Level" on page 409. **Default value:** Low 110; Medium 93; High 90
Error Percentiles	Displays the **Low**, **Medium**, and **High** adherence level percentile value that is used to calculate the error baseline threshold. For more details on this topic, see "Setting the Baseline Adherence Level" on page 409. **Default value:** Low 120; Medium 98; High 95
Good Boundary	Displays the actual value for the Good Boundary for each monitor measurement type. This is the value of a measurement that is not considered to be in error status, even though according to existing baseline percentiles it should report an error. For more details on this topic, see "Understanding the Good and Error Boundaries" on page 409. **Default value:** No value
All browsable monitor measurements	Displays the **Low**, **Medium**, and **High** adherence level percentile value that is used to calculate the warning and error baseline threshold for all browsable monitor measurements. **Default Warning values:** Low 110; Medium 93; High 90 **Default Error values:** Low 120; Medium 98; High 95

Activate Baseline Dialog Box

This dialog box displays a summary of the calculated monitor's baseline data, and enables you to save the current monitor configuration, view baseline measurement graphs, view failed operations, and activate baseline threshold configuration. For monitors that SiteScope is unable to calculate a baseline, it includes the reason for the failure.

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a group, or a monitor and select **Baselining** > **Review & Activate**.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit monitors** permissions can use the baseline feature to set monitor thresholds, and only for the monitors that are in the users allowed groups list. Monitors in groups for which the user does not have permissions are not displayed in the dialog box. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ To revert to the current monitor configuration, you must create a backup configuration before activating the baseline configuration. ➤ The amount of time required to activate the baseline threshold depends on the speed of the SiteScope server and the number of monitors selected for baselining. If SiteScope needs to restart before the activation process is complete, SiteScope automatically continues the process after the restart.
Relevant tasks	"How to Set Monitor Thresholds Using a Baseline" on page 418
See also	"Setting Status Thresholds Using a Baseline" on page 405

User interface elements are described below:

UI Element	Description
Successfully Calculated Monitors	
	**View Graph.** Displays a graphical representation of baseline data for all the measurements of the monitor. For details, see "Baseline Monitor Measurement Graphs Dialog Box" on page 504.
	**Select All.** Selects all listed monitors.
	**Clear Selection.** Clears the selection.
Monitor Name	Name of the SiteScope monitor selected for baselining.
Calculation Date	Date on which the baseline was calculated.
Error Status Reduction	Reduction in the number of error statuses for a monitor if the baseline threshold were applied. A negative number indicates an increase in the number of error statuses for a monitor if the proposed baseline thresholds were applied. **Example:** Suppose you manually configure the threshold status for CPU Utilization to Error if >= 65% and there are 5 error statuses for the CPU monitor (of which 3 errors are for data samples between 65%-70%, and 2 errors for above 70%). If you have SiteScope calculate the threshold using a baseline and the threshold is set to Error if >= 70%, Error Status Reduction would be 3. **Note:** The Error Status Reduction value is based on data collected on the calculation date. **Tip:** If more than three days have elapsed since the calculation date, we recommend that you recalculate the baseline.

UI Element	Description
Warning Status Reduction	Reduction in the number of warning statuses for a monitor if the baseline threshold were applied. A negative number indicates an increase in the number of warning statuses for a monitor if the proposed baseline thresholds were applied. **Example:** Suppose you manually configure the threshold status for CPU Utilization to Warning if >= 55% and there are 3 warning statuses for the CPU monitor (of which 2 warnings are for data samples between 55%-60%, and 1 warnings for above 60%). If you have SiteScope calculate the threshold using a baseline and the threshold is set to Warning if >= 60%, Warning Status Reduction would be 2. **Note:** The Warning Status Reduction value is based on data collected on the calculation date. **Tip:** If more than three days have elapsed since the calculation date, we recommend that you recalculate the baseline.
Failed Monitors	
	**Select All.** Selects all listed failed monitors.
	**Clear Selection.** Clears the selection.
Monitor Name	Name of the monitor for which SiteScope was unable to calculate a baseline.

UI Element	Description
Reason for Failure	Reason that SiteScope was unable to calculate a baseline value for the monitor. They include: ➤ **Insufficient data.** The monitor has not run for a sufficient period of time to collect data to produce a meaningful baseline threshold. This period depends on the **Minimum number of days required for baselining** and **Minimum number of samples required for baselining** settings in Infrastructure Preferences. For details on configuring the Baseline Settings, see "Baseline Settings" on page 735. ➤ **No measurements to baseline.** The monitor has no measurements that can be used in the baseline calculation. You cannot select the monitor for baseline activation. ➤ **No samples for the requested schedule.** No data samples were collected for the range schedule specified. You cannot select the monitor for baseline activation. ➤ **Unknown.** The reason for baseline calculation failure is unknown. You cannot select the monitor for baseline activation.
Can Be Activated	Indicates whether a baseline can be activated even if the monitor baseline calculation failed. Displays **No** if the baseline calculation failed for any reason other than **Insufficient data**. Displays **Yes** if the baseline calculation failed with the reason **Insufficient data**. SiteScope uses the limited measurement samples that were collected to calculate the baseline.

Backup Configuration Dialog Box

This dialog box enables you to save the current monitor threshold configuration before activating the baseline threshold. You use the Configuration Tool to restore the configuration settings. For details on the Configuration Tool, refer to the *HP SiteScope Deployment Guide* PDF.

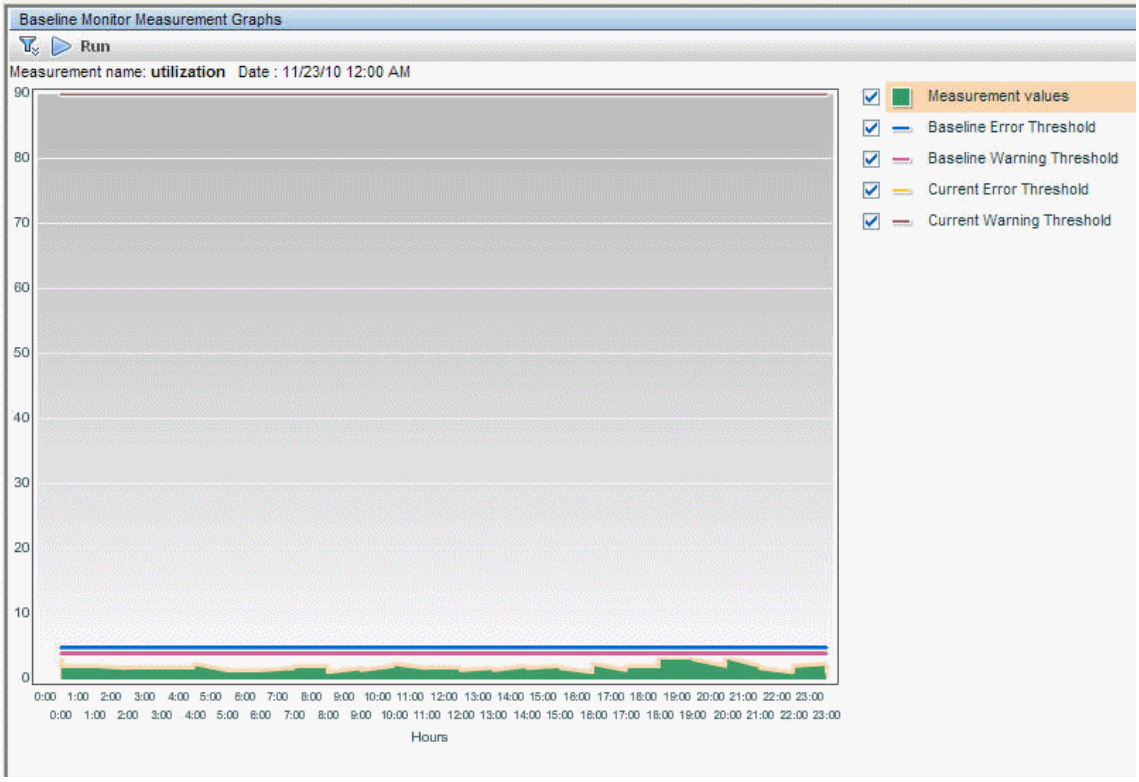
To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a group, or a monitor and select **Baselining** > **Review & Activate**. Click the **Backup Configuration** button.
Important information	Create a backup configuration before activating the baseline configuration, since you cannot undo threshold configuration changes after the baseline has been activated.
Relevant tasks	"How to Set Monitor Thresholds Using a Baseline" on page 418
See also	"Setting Status Thresholds Using a Baseline" on page 405

User interface elements are described below:

UI Element	Description
Enter target directory	Target directory where the backup configuration file is saved or use the default SiteScope installation directory. **Default value:** C:\SiteScope
Enter the backup file name	Name for the configuration backup file. By default, the file is named using the format: SiteScope_<MM_DD_YYYY>_<HH_MM_SS>. SiteScope saves a backup file in zip format to the specified location. **Example:** SiteScope__11_05_2008_08_24_06

Baseline Monitor Measurement Graphs Dialog Box

This dialog box displays a graph per measurement, for all the measurements of the monitor. The default date selected for displaying the graph is the day with the maximum error reduction. Each graph shows the current warning and error thresholds, the baseline warning and error thresholds, and historic data of all baseline-related monitor measurements over a 24-hour time period (from 00:00-23:59).



To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a group or a monitor container, and select **Baselining** > **Review & Activate**. In the **Successfully Calculated Monitors** pane, select a monitor with calculated baseline data, and click the **View Graph** button.
Important information	The data displayed in the monitor measurement graphs is an aggregate of the measurement data and as such, the time periods may not accurately reflect the time the data was collected.
Relevant tasks	"How to Set Monitor Thresholds Using a Baseline" on page 418
See also	"Setting Status Thresholds Using a Baseline" on page 405

Graph Settings

User interface elements are described below:

UI Element	Description
	**Annotaion Tool.** Creates a snapshot of the graph you are viewing and highlight important areas of the graph by drawing shapes, lines, and adding text to the snapshot. For user interface details, see "Annotation Tool" on page 1550.
 	**Collapse Report Filter.** Click to collapse or expand the report filter. **Tooltip:** When the collapsible report filter closes, the icon's tooltip displays details about the selections you made in the filter.

UI Element	Description
	**Run.** After you have specified the report setup, click to run the report for the date displayed in the date link.
Historic date <date link>	Opens the calendar, enabling you to select the date for which you want to create monitor measurement graphs. The calendar contains the following buttons: ➤ **Revert.** Returns to the previously selected report date. ➤ **Current.** Selects today's date in the calendar. ➤ **OK.** Updates the date link for the selected date and closes the calendar. ➤ **Cancel.** Closes the calendar without making any changes.

Graph Content

User interface elements are described below:

UI Element	Description
<Legend>	Describes the color coding used in the graph.
Measurement name	Name of the measurement appears above the graph.
Date	Time and date on which the graph was generated.
<Data points>	Displays for each 2 hour period of time on the **Time** axis, the value for the selected monitor measurement. **Tooltip:** The measurement value.
<Measurement Type> <y-axis>	Displays the monitor measurement type.

UI Element	Description
Hours <x-axis>	Time division units for the date specified when generating the report (from 0-24 hours).
Baseline Error Threshold	Displays the baseline threshold line that determines **Error** status. Measurements beyond this line exceed the error baseline status threshold for the monitor. This is displayed on the graph as a solid red line.
Baseline Warning Threshold	Displays the baseline threshold line that determines **Warning** status. Measurements beyond this line exceed the warning baseline status threshold for the monitor. This is displayed on the graph as a solid orange line.
Current Error Threshold	Displays the threshold line that determines **Error** status. Measurements beyond this line exceed the error status threshold for the monitor. This is displayed on the graph as a dashed black line.
Current Warning Threshold	Displays the threshold line that determines **Warning** status. Measurements beyond this line exceed the warning status threshold for the monitor. This is displayed on the graph as a dashed blue line.

Remove Baseline Dialog Box

This dialog box enables you to select the groups, monitors, or both from which to remove the baseline. You must remove a monitor's existing baseline calculation before you can recalculate the monitor's threshold baseline.

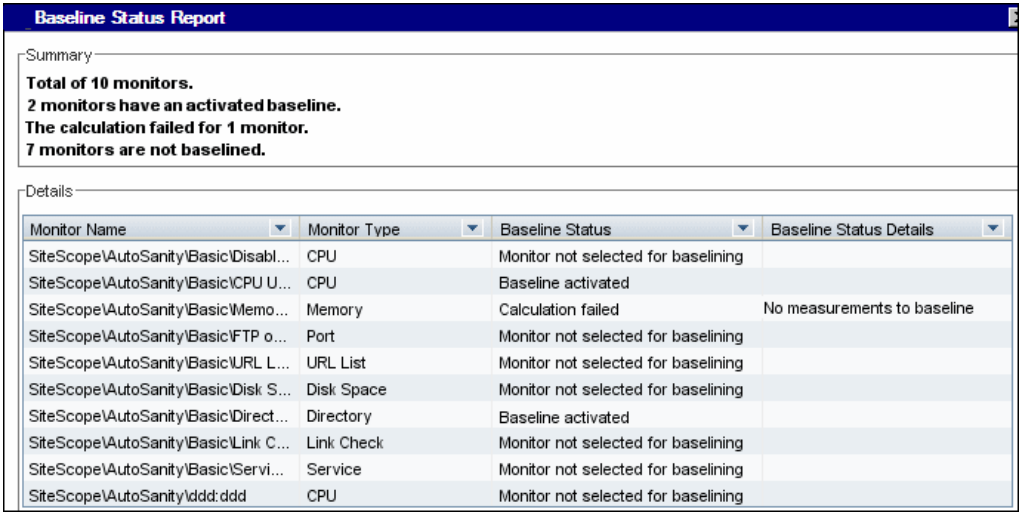
To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a group, or a monitor and select **Baselining** > **Remove**.
Important information	Only an administrator in SiteScope, or a user granted **Edit monitors** permissions can remove a baseline, and only for the monitors that are in the users allowed groups list. Monitors in groups for which the user does not have permissions are not displayed in the dialog box. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Set Monitor Thresholds Using a Baseline" on page 418
See also	"Setting Status Thresholds Using a Baseline" on page 405

User interface elements are described below:

UI Element	Description
<List of groups and/or monitors>	Groups, monitors, or both, from which you want to remove baseline threshold calculation. The list includes all groups and/or monitors in the currently selected container, and all child containers in the users allowed groups list. **Default value:** The current container and all child elements are selected.

Baseline Status Report

This report displays information about the baseline status for all monitors in the selected context.


Baseline Status Report

Summary

Total of 10 monitors.
2 monitors have an activated baseline.
The calculation failed for 1 monitor.
7 monitors are not baselined.

Details

Monitor Name	Monitor Type	Baseline Status	Baseline Status Details
SiteScope\AutoSanity\Basic\Disabl...	CPU	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\CPU U...	CPU	Baseline activated	
SiteScope\AutoSanity\Basic\Memo...	Memory	Calculation failed	No measurements to baseline
SiteScope\AutoSanity\Basic\FTP o...	Port	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\URL L...	URL List	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\Disk S...	Disk Space	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\Direct...	Directory	Baseline activated	
SiteScope\AutoSanity\Basic\Link C...	Link Check	Monitor not selected for baselining	
SiteScope\AutoSanity\Basic\Servi...	Service	Monitor not selected for baselining	
SiteScope\AutoSanity\ddd:ddd	CPU	Monitor not selected for baselining	

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a group, or a monitor and select **Baselining** > **Status Report**.
Important information	➤ This is an ad hoc report that is not saved to the SiteScope configuration data for later use. ➤ You can sort monitor types in ascending or descending order by clicking the column header. An arrow is displayed showing the sort order direction. ➤ You can filter the display for Monitor Type and Baseline Status by clicking the down arrow and selecting a monitor type or baseline status by which to filter. To clear the filter, select **(All)**.
Relevant tasks	"How to Set Monitor Thresholds Using a Baseline" on page 418
See also	"Setting Status Thresholds Using a Baseline" on page 405

User interface elements are described below:

UI Element	Description
Monitor Name	Name and path of the SiteScope monitor depending on the context. **Note:** Only monitors in groups or subgroups that a user has permissions to access are displayed in the report.
Monitor Type	The type of SiteScope monitor.
Baseline Status	The monitor's baseline status. The following statuses are available: ➤ **Monitor not selected for baselining.** The monitor has not been selected for baselining. ➤ **Calculating baseline.** SiteScope is in the process of calculating the baseline. ➤ **Calculation failed.** SiteScope was unable to calculate a baseline. ➤ **Calculated, not activated.** A baseline was calculated for the monitor, but it has not yet been activated. ➤ **Activating baseline.** SiteScope is in the process of activating the baseline. ➤ **Activation failed.** SiteScope was unable to activate the baseline. ➤ **Baseline activated.** The baseline has been activated for the monitor.

UI Element	Description
Baseline Status Details	Displays additional details for monitors with the following status: ➤ **Calculating baseline.** Displays the baseline calculation stage for the monitor. ➤ **Calculation failed**. Displays the reason that the baseline calculation failed (**Insufficient data**, **No measurements to baseline)**. Monitors that failed due to insufficient data are selected by default for automatic baseline calculation after the monitors have run for a period that is sufficient for SiteScope to accumulate data for the baseline period. For details, see "Activate Baseline Dialog Box" on page 499.
Refresh	Click during the calculation process to update the data in the status report.

13

Monitoring XML Documents

This chapter includes:

Concepts

Reference

Concepts

Monitoring XML Documents Overview

SiteScope's content matching capabilities is an important function in monitoring networked information systems and content. For SiteScope monitors that provide content matching, the basic content matching is available through the use of Perl regular expressions. SiteScope also includes the capability of matching document content by traversing XML documents. For example, you can include an XML match content string using the URL Monitor and Web Services Monitor to match an XML element name, an attribute of an XML element, or the content of an element. You can use this to check for content in XML based Web pages, SOAP or XML-RPC documents, and even WML pages served to WAP-enabled devices.

Reference

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.
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 **error** because the temperature value is 46, which is less than 72.

Part V

Integration Monitors

14

Working with SiteScope Integration Monitors

This chapter includes:

Concepts

Tasks

Reference

Concepts

Integration Monitors Overview

Integration Monitors are run by the SiteScope data collector and are used to capture and forward data from third-party applications (typically Enterprise Management Systems (EMS) applications and servers) into BSM.

Note: Access to Integration Monitor types requires that a special SiteScope Optional License be entered on the SiteScope server. For details, see "SiteScope Licenses" in the *HP SiteScope Deployment Guide* PDF.

You can create an EMS integration in BSM's EMS Integrations Administration page. For details, see "EMS Integration Administration" in *Solutions and Integrations* in the HP Business Service Management Documentation Library. When creating the integration, the step to create monitors opens System Availability Management (SAM) to enable you to create the SiteScope Integration monitors.

There are two levels of configuration for collecting the data and forwarding that data to BSM:

- **Required:** The monitors must be configured to properly map to the monitored system and collect the required samples, whether in the form of events, metrics, or tickets. The field mapping from the monitored system is done by selecting a sample type in the Field Mapping setting and editing the corresponding script template in a text editor.
- **Optional:** The data can also be mapped to a topology to forward data to the correct CI hierarchy in BSM. This enables the monitor to accurately report status to the required CIs within BSM for use by the different applications in the product. The topology settings are configured using a topology script that is loaded depending on the type of topology you want to create.

This section also includes:

➤ "Integration Monitor Categories" on page 523

➤ "Field Mapping Sample Types" on page 525

Integration Monitor Categories

Integration monitors can be divided into two categories.

Application-Specific Monitors

These integration monitors are designed for use with specific EMS applications. These monitors are predefined with the required field mapping and topology settings.

The monitors include:

➤ HP OM Event Monitor. For details, see the *Monitor Reference* guide in the SiteScope Help.

➤ HP Service Manager Monitor. For details, see the *Monitor Reference* guide in the SiteScope Help.

➤ NetScout Event Monitor. For details, see the *Monitor Reference* guide in the SiteScope Help.

The scripts for both the field mapping and the topology settings can be further configured to suit the needs of your specific environment.

Note:

- The HP OM Event monitor is not available when SiteScope is connected to BSM version 9.00 or later (unless the monitor was created in an earlier version of SiteScope that was upgraded to SiteScope 11.10). OM events can be forwarded to BSM 9.00 from the HPOM Server, provided you have an Event Management Foundation license and an integration is configured per the instructions in the *HP Business Service Management Deployment Guide* PDF in the HP Business Service Management Documentation Library.
- Topology Settings are not available for the NetScout Event Monitor.

Generic Integration Monitors

Technology Integration Monitors designed for use with most EMS applications that support extraction of data from a database, log file, SNMP trap, or Web service interface.

The field mapping and topology settings for these monitors must be configured by loading the applicable scripts and editing them in a separate text editor during monitor creation.

The monitors include:

- Technology Database Integration Monitor. For details, see the *Monitor Reference* guide in the SiteScope Help.
- Technology Log File Integration Monitor. For details, see the *Monitor Reference* guide in the SiteScope Help.
- Technology SNMP Trap Integration Monitor. For details, see the *Monitor Reference* guide in the SiteScope Help.
- Technology Web Service Integration Monitor. For details, see the *Monitor Reference* guide in the SiteScope Help.

Field Mapping Sample Types

The integration monitors use field mapping scripts to correctly map the data they collect to a format recognizable by BSM. For the generic integration monitors, you configure and customize these mappings as required. When you select a field mapping type, you can use the script editor provided, or you can copy the script into your preferred text editor, make your changes, and then copy the script back into the field mapping text box.

Tip: The mappings for the application-specific monitors are not editable while configuring the monitor. We recommend that you use the out-of-the-box integration mappings already configured for those monitors.

When configuring the generic integration monitors, select from the following types of sample scripts:

- **Metrics.** Used to collect time-based data. Data collected by Integration Monitors that use the metrics sample type is integrated into BSM as typical SiteScope data and can be viewed in all contexts that support viewing SiteScope data (for example, Service Health, Service Level Management, SAM, user reports, and so on).
- **Events.** Used to collect data on specific events. Data collected by Integration Monitors that use the event sample type is integrated into BSM using the UDX framework and can be viewed in contexts that support the display of UDX data (Event Log, Service Health, trend reports). The data can also be accessed using the BSM API.

  Note: Events sent by EMS applications are event samples. They are not the same as Operations Management events in BSM.

- **Tickets**. Used to collect incidents and events from ticketing systems. Data collected by integration monitors that use the ticketing sample type is integrated into BSM and can be viewed in Service Health and Service Level Management.

The Database, Log File, SNMP Trap, and Web Service Technology Integration Monitors can be configured to work with these sample types. You use the field mapping script templates that come prepackaged with SiteScope as a basis for creating a customized configuration required for your specific environment. When you configure an integration monitor, you select the sample type to load the required script template and edit the script to collect the data you want to forward to BSM.

For details on customizing the field mapping scripts, see "Integration Monitor Field Mapping" on page 547.

Topology Settings for Technology Integration Monitors

To establish the full integration with BSM, you can select a topology template for your integration monitor. You do this while creating an integration monitor in the Topology Settings area. The topology templates for **Node, Node - Running Software**, and **Tickets** are specially configured with the necessary values to forward data to the required CIs in BSM's RTSM.

Note:

- The script for EMS topology templates from SiteScope 10.x is displayed in SiteScope in the previous content language format, even if SiteScope is connected to BSM 9.00. For example, CI Type host appears in the script instead of node.
- If SiteScope is connected to BSM versions earlier than 9.00, the **Hosts** and **Host-Software elements** topology script templates are displayed in the topology template script list for the monitor instead of **Node** and **Node - Running Software**.
- You cannot customize organization topology for the NetScout Event or HP Service Manager monitors.

The topology is written as a topology script, using Jython—a language based on Python and powered by Java. For details on how to work in Jython, you can refer to these Web sites:

- http://www.jython.org
- http://www.python.org

The script includes the basis of the functions necessary to retrieve the required topology data from the monitored application. To build the topology, the script uses the sample that was created as a result of the monitor's field mapping. The script includes the mapping to forward the retrieved data to the relevant CIs in BSM.

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 RTSM.
- If there were any changes to any of the CI's properties.
- The initial monitor run after SiteScope is restarted.

This prevents overloading the RTSM with CI updates coming from the monitor.

This section also includes:

- "Selecting a Topology" on page 529
- "Editing the Topology Script" on page 532
- "Topology Script Properties File" on page 534
- "Additional Documentation" on page 534

Selecting a Topology

When working with application-specific monitors, you do not select a topology and the topology is preconfigured with the necessary data for the integration.

When working with generic integration monitors, you can select from the following topology settings:

➤ **Custom**. You create your own topology if you want the retrieved data to be forwarded to specific CIs and not the standard Node or Running Software CIs.

Note: You must be familiar with the Jython language if you select **Custom**, since no topology script is loaded and you must write the topology script in Jython yourself. We recommend that you begin with either **Node** or **Node - Running Software** and edit one of those scripts.

➤ **Node**. Creates a Node CI with an EMS monitor CI as a leaf node.

➤ **Node - Running Software**. Creates a topology with a Node CI as the parent CI and a Running Software CI under it, and an EMS monitor CI under the Running Software CI. If your subject as defined in the field mapping is system, a topology of a Node CI and an EMS monitor CI under is created.

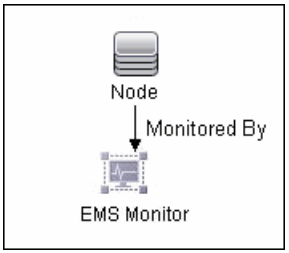
➤ **Tickets**. Creates a BusinessService CI with an EMS monitor CI as a leaf node.

Note: The topology script must include the EMS monitor CI as the lowest leaf in the topology created by the integration.

For more information on the default integration types, see "Understanding Node, Tickets, or Node - Running Software Integration Types" in *Solutions and Integrations* in HP Business Service Management Documentation Library.

Node Topology

The default topology created includes a Node CI with an EMS Monitor CI as its leaf node.



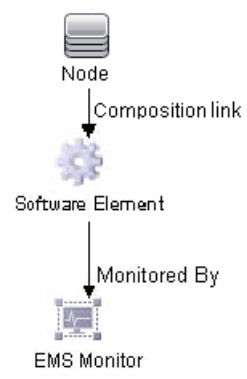
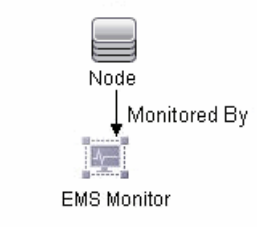
The Node CI has a monitored by relationship with the EMS Monitor CI. The EMS Monitor CI passes status onto the Node CI.

Node - Running Software Topology

In this topology, there are two types of data that can be retrieved from the monitored system: **Software element** events and **system** events.

- **Software element events**. This data is recognized as data affecting services or applications. These events are mapped to the system KPI for the relevant CIs. These events are not propagated to the Node CIs.
- **System events**. This data is all other data retrieved from the monitored application that does not affect services or applications. This data passes status onto the Node CI. The status may propogate to the Application CI if there is a relationship between the Node CI receiving the system event and the Running Software CI. This event is also mapped to the system KPI for the relevant CIs.

The following table illustrates the topology created for each type of event:

Topology Created for Software Element Event	Topology Created for System Event
	

If the events do not belong to the category of service events, then the event is considered a system event.

You can configure which data is considered application or service data and which data is not. You configure these instructions by editing the topology script as follows:

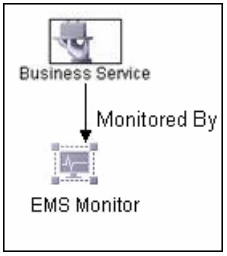
Search for the following string in the topology script:

if (subject != "system"):

The variable **subject** represents the subject field in the retrieved sample (as defined in the field mapping for events). The value **system** is an example of possible values representing the data from an application that is considered 'system' data and not forwarded to the Running Software CI. This 'system' data is forwarded to the Node CI.

Tickets

The default topology created includes a BusinessService CI with two EMS monitor CIs; one that monitors the running software and the other that monitors the node. The BusinessService CI has a monitored by relationship with the EMS Monitor CI.



The EMS Monitor CI passes status onto the BusinessService CI.

Editing the Topology Script

To configure the topology, you must edit the topology script that appears in the Topology Settings area when creating an integration monitor. You can edit the script in the Topology Settings field using the script editor provided by SiteScope.

The **Node**, **Node - Running Software**, and **Tickets** topologies are already configured with the necessary information. Following are the guidelines for editing the script if you want to create your own topology.

- We recommend that you familiarize yourself with the Jython language before attempting to edit this script.
- The Jython language is sensitive to spaces and tabs and you must be careful while editing the script.
- You must leave the import section as is and only add to it.
- The main body of the script is mandatory and consists of:

  ```
  def DiscoveryMain(Framework)
  ```

  This main function is responsible for creating Object State Holder Vector (OSHV) results. This holds the CI data and how to map the incoming samples to the CIs.

- Each CI should have only one EMS Monitor CI as a leaf node.
- For event scripts, the following expressions must appear as the last lines in the script:

  ```
  Framework.setUserObject("result_object",monitoredCiType)
  return OSHVResult
  ```

  The variable monitoredCiType is the CI type being monitored by the EMS Monitor CI that receives the event.

  If the script creates more than one EMS Monitor CI for one retrieved event, you must determine to which of the CIs that event belongs and passes status. You do this by assigning the correct value to the monitoredCiType. For example, if the script creates one EMS Monitor CI for an Application CI and one for a Node CI, and you want the event to pass status to the Node 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.

Topology Script Properties File

The <**SiteScope root directory**>**discovery****discovery_agent.properties** file controls many aspects of the topology script. Generally, you do not need to edit this file. It already includes all the properties necessary for running the topology script.

If you working in a secure BSM 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 **discovery_agent.properties**, you must restart SiteScope to enable your changes to take effect.

Additional Documentation

For general information on topology scripts, see "Create Jython Code" and "Developing Jython Adapters" in *RTSM Developer Reference Guide* in the HP Business Service Management Documentation Library.

For information about Java classes that can be used in topology scripts, see "HP Data Flow Management API Reference" in *RTSM Developer Reference Guide* in the HP Business Service Management Documentation Library.

Tasks

How to Deploy Integration Monitors

Note: You can deploy integration monitors while working in:

- A standalone SiteScope that reports to BSM
- Directly in SAM Admin
- BSM's EMS Integrations Administration which opens SAM Admin

This task describes the steps involved in deploying an integration monitor.

This task includes the following steps:

- "Plan your integration" on page 536
- "Select a SiteScope" on page 536
- "Create a group for the integration monitor" on page 536
- "Configure the integration monitor" on page 537
- "Edit indicator mappings in BSM (for metrics flow)" on page 538
- "Edit field mappings and topology script" on page 539
- "Configure the EMS Integrations application in BSM" on page 540

1 Plan your integration

For details, see the introduction and the first 3 steps in "How to Integrate Data from Third-Party Sources (EMS Data) into HP Business Service Management" in *Solutions and Integrations* in the HP Business Service Management Documentation Library.

2 Select a SiteScope

Select the SiteScope server from which you want to deploy the integration monitor:

- For SiteScope standalone, select and open a SiteScope instance.
- When in SAM Admin, select the SiteScope server from which you want to deploy the integration monitor. For user interface details, see "System Availability Management Administration Page" in *Using System Availability Management* in the HP Business Service Management Documentation Library.
- When in EMS Integrations Administration, click the **New Integration** or **Edit Integration** button. In the Edit Integration dialog box, click the link in the **System Availability Management** pane to open SAM Administration window where you can select a SiteScope server. For user interface details, see "Edit Integration Dialog Box" in *Solutions and Integrations* in the HP Business Service Management Documentation Library.

3 Create a group for the integration monitor

We recommend that you create special groups for the integration monitors. This enables you to more easily recognize the data that is reported to BSM as coming from the integrations.

For user interface details, see "New SiteScope Group Dialog Box" on page 387.

4 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 OM Event Monitor (for details, see the *Monitor Reference* guide)
- HP Service Center Monitor (for details, see the *Monitor Reference* guide)
- NetScout Event Monitor (for details, see the *Monitor Reference* guide)

You can choose from the following generic integration monitors:

- Technology Database Integration Monitor (for details, see the *Monitor Reference* guide)
- Technology Log File Integration Monitor (for details, see the *Monitor Reference* guide)
- Technology SNMP Trap Integration Monitor (for details, see the *Monitor Reference* guide)
- Technology Web Service Integration Monitor (for details, see the *Monitor Reference* guide)

5 Edit indicator mappings in BSM (for metrics flow)

You can also choose indicators in BSM and map them to third-party metrics.

a In BSM, create an indicator assignment for a new monitor type which is the type of the EMS synthetic monitor that will be defined in the field mapping. For task details, see "How to Create and Manage Indicator Assignments" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

Example:

If the synthetic monitor type is MyDiskMonitorType, create a new monitor type, MyDiskMonitorType and in the New Assignment dialog box for the MyDiskMonitorType monitor, enter diskFull for the metric pattern (this is the metric name that will be defined in the field mapping). Select the indicator to which you want to map this metric, for example, Disk.

Note: That you should choose an indicator that is applicable for the Computer CI type.

b After defining indicator mappings, click **Publish changes** to publish the indicator mappings to SiteScope.

c In SiteScope, create an integration monitor instance, and load the **Metrics** sample type.

d In the **Field mapping** section, for example, enter using the following:

```
MonitorName="MyMonitor"
TargetName="ServerName"
MonitorState="Disk is almost full"
MonitorType="MyDiskMonitorType"
MeasurementName(1)="diskFull"
Value(1):DOUBLE=90.0
```

e Click **Save**. The correct indicator is sent in the topology and data, according to the defined mapping for the synthetic monitor.

6 Edit field mappings and topology script

For generic integration monitors or any special customizations, you must also:

➤ Select the sample field mapping script (**Events**, **Tickets, Metrics**), and edit to suit your organization's needs. The mapping defines the processing of incoming data and the output sample forwarded to BSM. For concept details, see "Integration Monitor Field Mapping Overview" on page 548.

➤ Select a topology script template and edit the topology settings. For concept details, see "Topology Settings for Technology Integration Monitors" on page 527.

The topology script templates that are available depend on the field mapping selected.

Events Sample Script	Tickets Sample Script	Metrics Sample Script
Select one of the following options: ➤ **Node** to create the Node and EMS Monitor CIs ➤ **Node-Running Software** to create the Node, Running Software, and EMS Monitor CIs ➤ **Custom** to create the CIs according to the topology user-written topology script	Select one of the following options: ➤ **Ticket** to create the Business Service and EMS Monitor CIs ➤ **Custom** to create the CIs according to the topology user-written topology script	Select one of the following options: ➤ **SiteScope Topology** to create the basic SiteScope topology with Sitescope Monitor and Computer CIs ➤ **No topology** to send only data without topology ➤ **Custom** to create the CIs according to the topology described in user-written topology script

7 Configure the EMS Integrations application in BSM

Note: If you are configuring a metrics integration, do not need to go to BSM's SAM Admin and configure a new integration. You just need to create a monitor and select the **Report topology** option.

In addition to configuring the monitor, you need to configure the EMS Integrations application in BSM. For details, see the remaining steps from the "Create or customize a data assignment" step in "How to Integrate Data from Third-Party Sources (EMS Data) into HP Business Service Management" in *Solutions and Integrations* in the HP Business Service Management Documentation Library.

Reference

List of Deprecated Integration Monitors

The following table lists the deprecated Integration Monitors, and the respective Technology Integration Monitors that can replace them:

Deprecated Monitor	Recommended Monitor
Avalon Event	Technology SNMP Trap
BMC Patrol Event	Technology SNMP Trap, Technology Log File
BMC Patrol	Technology Log File
CA Unicenter Event (1)	Technology SNMP Trap
Compaq Insight Manager Event (2)	Technology Database
HP Systems Insight Manager Event	Technology Database
Netcool Event	Technology SNMP Trap
NetIQ (3)	Technology Database
Remedy Ticketing	Technology Database
Tivoli TEC Event	Technology Database
Tivoli DM	Technology Database
WhatsUp Event (4)	Technology Log File

The following are examples of how a Technology monitor can be configured to replace a deprecated monitor:

(1) Configure CA Unicenter agents to send SNMP traps to a SiteScope host machine where a Technology replacement monitor has been configured.

(2) For Compaq Insight Manager version 7.0, configure the replacement SiteScope monitor to read from the following tables: Notices, NoticeType, Devices, StringResource, and StringTableLarge.

(3) For NetIQ versions 5.0 and 5.1, configure the replacement SiteScope monitor to query tables Data (contains raw data) and DataHeader (contains metadata about the objects that NetIQ monitors).

(4) For WhatsUp version 8.0, configure the replacement SiteScope monitor to read from the log file EV-<date>.tab.

Note: Beginning with SiteScope 8.x, the monitor configuration file **main.config** is no longer used. All functions that were supported in **main.config** are now supported in **event.config** and available in the **Fields Mapping** setting.

Troubleshooting and Limitations

This section describes troubleshooting and limitations when working with SiteScope Integration Monitors.

- "Integration Monitor Logs" on page 543
- "Other Log and Troubleshooting Issues" on page 544
- "Additional Troubleshooting Information" on page 545

Integration Monitor Logs

Integration Monitor activity is logged to <**SiteScope root directory**>**logs****RunMonitor.log** and <**SiteScope root directory**>**logs****bac_integration****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 BSM.
- 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 BSM 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****bac_integration.log**.
- If samples are created and sent from SiteScope but cannot be seen in BSM Service Health, Event Log, or SiteScope reports, search for the string ERROR or WARN in the **wde.logl** and **loader.logl** files in the <**BSM root directory**>**log****mercury_wde**\ directory to make sure the samples were not dropped due to missing fields or values.
- Increase the level of Service Health logging in <**BSM root directory****conf****core****Tools****log4j****EJB****ble.properties** file to verify that Service Health 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 <**BSM root directory****log****EJBContainer****TrinitySamples.log**.

Tip: After you have determined the cause of the problem, we recommend that you set log levels to their default settings so as not to overload the system.

Additional Troubleshooting Information

Additional troubleshooting information is located in the HP Software Self-solve knowledge base (http://h20230.www2.hp.com/selfsolve/documents) (you must log on to the knowledge base with your HP Passport ID) and in the following sections of the documentation:

- For Technology Database Integration monitor, see "Troubleshooting the Technology Database Integration Monitor" in the *Monitor Reference* guide.
- For Technology Log File monitor, see "Troubleshooting the Technology Log File Integration Monitor" in the *Monitor Reference* guide.
- For Technology SNMP Trap monitor, see "Troubleshooting the Technology SNMP Trap Integration Monitor" in the *Monitor Reference* guide.
- For Technology Web Service Integration monitor, see "Troubleshooting the Technology Web Service Integration Monitor" in the *Monitor Reference* guide.

15

Integration Monitor Field Mapping

This chapter includes:

Concepts

Reference

Concepts

Integration Monitor Field Mapping Overview

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 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 BSM.

Integration Monitors designed for use with specific EMS applications (these currently include HP OM, HP Service Center, and NetScout) can be configured without editing their field mapping script. The mappings are predefined by HP and require modification only if specific customizations are required. For details on editing these field mapping scripts, see the description for the field mapping element in the user interface pages for the monitor you are deploying.

For Technology Integration Monitors (Technology SNMP Trap, Technology Log File, and Technology Database monitors), you must select the sample type and the required script template is loaded directly into the field mapping text box. You must edit the field mapping script to suite your organization's needs. The Technology Web Service Integration Monitor field mapping may also need to be customized.

You can select from the following sample types:

➤ **Events**. Select to forward event data to BSM.

When you select **Events** and you want to integrate to BSM using topology settings, you can select from the following topology script templates: **Node**, **Node - Running Software**, or **Custom** (only if you are familiar with the Jython language, since you must write the Jython topology script yourself).

Note:

➤ Events sent by EMS applications are event samples. They are not the same as Operations Management events in BSM.

➤ When SiteScope version 11.10 or earlier is connected to BSM 9.00, the **Hosts-Applications** topology script template is no longer available in the topology template script list for the monitor. Only existing integrations that report **Hosts-Applications** (created in SiteScope connected to BSM 8.x) continue reporting to BSM 9.00. You cannot create new integrations using this script template type.

➤ **Metrics**. Select to forward metrics data to BSM.

When you select **Metrics** and you want to integrate to BSM using topology settings, you can select from the following topology script templates:

➤ **SiteScope Topology.** Select to send SiteScope topology (monitors). This is the default setting. SiteScope reports this data to the Computer CI, a sub-type of the Node CI.

➤ **No Topology**. Select if you do not want to send any topology (although data and configuration samples are still be sent).

➤ **Custom.** Enables you to create your own topology. You must be familiar with the Jython language, since you must write the Jython topology script yourself.

Note: SiteScope uses indicator definitions for custom EMS synthetic monitors that are defined in BSM (and that are applicable for Computer CI type). If a different ETI has be specified in the monitor's field mapping, this overrides the default indicator definition.

➤ **Tickets**. Select to forward ticket data to BSM.

When you select **Tickets** and you want to integrate to BSM using topology settings, you can select the following topology script template: **Tickets** or **Custom** (only if you are familiar with the Jython language, since you must write the Jython topology script yourself).

For details, on selecting a topology setting, see "Topology Settings for Technology Integration Monitors" on page 527.

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 metrics 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 BSM or discard). No further sections are checked after the first match. If no matches are found, the event is discarded.

In addition to the event handlers, the field mapping can contain special entries that affect the integration monitor engine as a whole. These values are grouped into the [$DEFAULT_PARAMETERS$] section. This section defines default values for tags that are common for all handlers. Any tag can be set in this section of the field mapping. It is used to create a reported value unless overridden in the matched event handler. For each incoming event, this event handler is always run prior to the matched event handler.

For details on event handler structure, see "Event Handler Structure" on page 568.

Reference

Configuring Field Mapping for Event Samples

The events sample type is used for extracting events collected by external systems and importing them to BSM. 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 also includes:

Mandatory Values for the Event Script

The table below lists mandatory values for the event script.

Field Name	Type	Description	Example
time_stamp	DOUBLE	Time stamp in seconds since Jan 1 1970.	time_stamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS"). time_stamp:DOUBLE=time()
severity	INT	Can be one of the following preconfigured severities (based on applicable integer): 0:SEVERITY_UNKNOWN 1:SEVERITY_INFORMATIONAL 2:SEVERITY_WARNING 3:SEVERITY_MINOR 4:SEVERITY_MAJOR 5:SEVERITY_CRITICAL	severity:INT=SEVERITY_MINOR
target_name	STRING	Name of device or host that generated the event.	target_name=$hostName target_name=resolveHostName (String host name)
status	STRING	Status of event in external EMS terminology.	status="OPEN" status="ASSIGNED" status="CLOSED"
subject	STRING	Subject of event (e.g. CPU, SAP application, Hard Disk), middle/high level hierarchy describing the event source.	subject="DISK"

Field Name	Type	Description	Example
instance	STRING	Instance of subject that generated the event (e.g D:\). Lowest level of hierarchy describing the event source.	instance="E:\\"
description	STRING	Textual description of event.	description="free space on drive e is below 10%"
data_source	STRING	System that generated the event.	data_source="HP OVO"

Optional Values for the Event Script

The table below lists optional values for the event script.

Field Name	Type	Description	Example
target_ip	STRING	IP of host or device that generated the event.	target_ip=$IPString
object	STRING	Optional level in the hierarchy describing the event source.	object="OS"
event_id	STRING	Unique identifier of this event.	event_id=$id
logical_group	STRING	Logical grouping of this event.	logical_group="error messages"
monitor_ group	STRING	Monitor group that reported this event.	monitor_group="log monitors on \\hostname"
orig_severity_ name	STRING	Severity in external EMS terminology.	orig_severity_name ="Cleared"
acknowledged _by	STRING	Name of user that acknowledged this event.	acknowledged_by =$username
owner	STRING	Name of user who owns this event.	owner="admin"

Field Name	Type	Description	Example
value	DOUBLE	Use to transfer numerical values from the event.	value=$thresholdViolated
attr1	STRING	Extra data slot.	attr1=$history
attr2	STRING	Extra data slot.	attr2=$moreHistory
attr3	STRING	Extra data slot.	attr3="Design"
attr4	STRING	Extra data slot.	attr4=$MonitorOutput
attr5	STRING	Extra data slot for long strings.	attr5=$Longhistory

Host DNS Resolution for Event Sample

Both the FQDN (fully qualified domain name) and valid IP address are necessary for the fields that are used to create Node CIs in the BSM integration.

If you do not know the FQDN, IP address, or both, 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, IP address, or both, are 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, IP address, or both, 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 Metrics Samples

The metrics sample type is used for extracting metrics collected by external systems and importing them to BSM. When configuring an integration monitor's field mapping, select the **Metrics** sample type to load the metrics 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 also includes:

- "Mandatory Values for the Metrics Script" on page 559
- "Optional Values for the Metrics Script" on page 560
- "Metrics Script Example" on page 562

Mandatory Values for the Metrics Script

The table below lists mandatory values for the metrics 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 metric.	MeasurementName(1)="CPU Temperature"
Value(N)	DOUBLE	Value of Nth metric.	Value(1):DOUBLE=$CPU Temperature

Optional Values for the Metrics Script

The table below lists optional values for the metrics script.

Field Name	Type	Description	Example
Measurement ETI	STRING	The display name of the ETI. **Note:** When using BSM 9.00, add the relevant indicator names to the integration field mapping (otherwise the system KPI is used instead), or configure the indicator in SAM Admin. For details, see "Indicator Assignment Settings" in *Using System Availability Management* in the HP Business Service Management Documentation Library.	MeasurementETI(1)= "Indicator display name"

Field Name	Type	Description	Example
Measurement CI Hint	STRING	CI resolution hint that is used to identify monitored CIs and relate metrics to them. SiteScope sends an out-of-the-box CI resolution hint in the format based on the monitor's internal IDs. For EMS metric field mapping, you might want to send a custom CI resolution hint when: ➤ Sending a custom topology without monitor CIs using a custom topology script. ➤ You only want to forward third party metrics and connect them to an existing topology. In this case, you create a field mapping, provide CI resolution hints, and select the **No Topology** option in the integration monitor's Topology Settings. The CI resolution hint must be specified in a format recognizable in BSM, as set out in the note below.	MeasurementCIHint(1)= "@@SCDAM038.testlab"

Note: You can use the following formats for CI resolution hints:

1 **Standalone CIs that do not exist in the context of Node CIs.** For example, Business Application, Business Service, or Siebel Enterprise. CI resolution hint should be a CI name.

Example For a Business Service CI named myBusinessService, the CI resolution hint would be: MeasurementCIHint(1)="myBusinessService". Note that the CI name must be unique in RTSM.

2 **Node topology.** CI resolution hint should be a fully qualified domain name or an IP address of a node that follows the @@ separator.

Example: To report a node with IP address 12.34.56.78, the CI resolution hint would be: "@@12.34.56.78" or "@@<MachineName>".

3 **CIs which exist in the context of Node CIs.** For example, CIs which belong to CI types that inherit from Running Software, Node Element, or Network Entity. You must specify in the hint both the Node CI and the CI connected to the Node CI, separated by @@:

Example: For an Oracle Database CI connected to the Node CI, the CI resolution hint should be in the format: "<oraclesid>:<product name>@@<fqdnhostname>".

Metrics Script Example

In the example below, two metrics are sent: the first one (MeasurementName (1)) takes its name from the $legend field and takes the value from the $value field. A second metric (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 Service Management #
##########################################
[$DEFAULT_PARAMETERS$]
# 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 metric in the script, a separate sample is sent with each of the metrics.

Note: When specifying multiple metrics per file, the metric 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 BSM. 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 also includes:

- "Mandatory Values for the Ticket Script" on page 565
- "Optional Values for the Ticket Script" on page 566
- "Conditional Expression Example" on page 567
- "Ticket Script Example" on page 567

Mandatory Values for the Ticket Script

The table below lists mandatory values for the ticket script.

Field Name	Type	Description	Example
time_stamp	DOUBLE	Time stamp in seconds since Jan 1 1970.	time_stamp:DOUBLE=str_to_seconds($time,"yyyy-MM-dd HH:mm:ss.SSS").
severity	INT	Can be one of the following preconfigured severities (based on applicable integer): SEVERITY_UNKNOWN SEVERITY_INFORMATIONAL SEVERITY_WARNING SEVERITY_MINOR SEVERITY_MAJOR SEVERITY_CRITICAL	4".equals($severity) ? "Low" : ("3".equals($severity) ? "Average" : ("2".equals($severity) ? "High" : ("1".equals($severity) ? "Critical" : "Unknown")))
target_name	STRING	Name of the entity (usually a service) that generated the ticket.	target_name="mail service" (Do not enter static string here, should be retrieved dynamically from the ticket.)
data_source	STRING	System that generated the ticket.	data_source="ticketing" (This string should not be edited for HP ServiceCenter integration and must be edited for a generic technology integration monitor.)
ticket_id	STRING	ID of the ticket.	ticket_id=112233
ticket_state	STRING	One of the states in the incident lifecycle as defined in the ticketing system.	"Open" / "Closed"

Field Name	Type	Description	Example
ticket_type	STRING	Type of the incident as defined in the ticketing system.	"Incident"
orig_severity_name	STRING	Severity in external EMS terminology.	orig_severity_name ="Cleared"

Optional Values for the Ticket Script

The script includes comments describing the optional values available for the ticket script. They include those listed here:

Field Name	Type	Description	Example
subject	STRING	Middle/High level hierarchy describing the event source.	CPU, SAP application, hard disk
instance	STRING	Instance of subject that generated the event. The lowest level hierarchy describing the event source.	D:\ \
object	STRING	Optional level in the hierarchy describing the ticket source.	object="OS"
logical_group	STRING	Logical grouping of this ticket.	logical_group="error messages"
monitor_group	STRING	Monitor group that reported this ticket.	monitor_group="log monitors on \\hostname"
elapsed_time	STRING	Elapsed time of the ticket.	
orig_severity_name	STRING	Severity name as defined in the ticketing system.	
attr1	STRING	Extra data slot.	attr1=$history
attr2	STRING	Extra data slot.	attr2=$moreHistory

Field Name	Type	Description	Example
attr3	STRING	Name of organization which owns a business service (if used in the Business Service integration topology flow).	Attr3="XYZ Inc"
attr4	STRING	Type of organization which owns a business service (if used in the Business Service integration topology flow).	Attr4="department"
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 BSM.

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 permitted in the field mapping. The comment starts with either **#**, **!**, or **;** character and continues to the end of the line.

Note: Use only the mandatory and optional fields defined in the script templates when working with the field mapping. See the tables in the following sections for more information.

This section also includes:

Matching Condition

The Match Condition must be a valid boolean expression. The expression can contain calls to the operators and functions defined below. The expression can access the contents of the event that is being processed using the dollar sign ($) notation. For example, if the incoming event is SNMP Trap, then its enterprise OID can be accessed as $oid. For names specific to a monitor, refer to the documentation of the relevant monitor type.

Note: The Match Condition expression is limited to 4,000 characters.

The matching condition has the form:

```
$MATCH=Boolean expression
```

where the Boolean expression is one of the expressions listed in the table below. When mentioned in the description, the expression can also be used to assign values into tags (see "Tags" on page 574).

Expressions and Functions	Description	Examples	True if
<, <=, >, >=, ==, !=	Checks the numerical correctness of the expression. Can be used with INT or DOUBLE fields.	$MATCH= $numberOfLines == 100	$numberOfLines equals 100
		$MATCH= $numberOfColumns <= 107	$numberOfColumns equals 107 or less
equals(String)	Checks for string equality.	$MATCH= "ERROR".equals($status)	$status equals the word ERROR
		$MATCH= $status.equals("ERROR")	$status equals the word ERROR

Expressions and Functions	Description	Examples	True if
true, false	Constant Boolean values.	$MATCH= true	always true.
&&, ||	To be used to combine any of the above boolean expressions.	$MATCH= $status.equals ("ERROR") || $numberOfLines == 100	$status equals the word ERROR or if $numberOfLines equals 100
time()	Returns the current time, in seconds, since January 1, 1970 format. Can be used with DOUBLE fields.	$MATCH= $timeStampField > (time()-600)	the value of the $timeStampField is newer 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 make 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 host name)	Performs DNS resolution from a server to its IP address. If the DNS resolution fails, the function returns the value unknown host.	target_ip= resolveHostIP ($host)	
resolveHostName (String host name)	Performs DNS resolution from an IP address to a fully qualified domain name. If the DNS resolution fails, the function returns the originally input host name.	target_name= resolveHostName ($host)	

Any of the above expressions can be used and the expression can refer to incoming event fields. The value of the expression, which can be either **true** or **false**, determines whether the event handler is be used to process the event or not.

Basic String Expressions

The following table summarizes the string expressions that can be used in the field mapping:

Operation	Description	Examples
+	String concatenation.	"trap type is " + $trap
substring	Substring of given string.	$var4.substring(3,5)
indexOf	Return indexOf string in another string.	$var4.indexOf($var3)

Basic Conditional Expression

One conditional expression is supported; the **?** operator. This operator can be used to compose three expressions into one (for example, <Conditional part> ? <if true part> : <if false part>).

Action Directive

The action directive has the form:

$ACTION= TOPAZ_BUS_POST or DISCARD

The value of the Action directive defines whether the event is processed and forwarded to BSM, 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 BSM bus and database.	BSM
TOPAZ_BUS_POST (ss_t)	Send the metrics to RTSM as SiteScope Data.	BSM
DISCARD	Do not send the data to BSM.	events you want to filter out

Note: If you are using the metrics mapping, TOPAZ_BUS_POST(ss_t), the data is sent to the BSM database as SiteScope data, and thus saved to the database. For details on metrics mapping, see "Configuring Field Mapping for Metrics Samples" on page 558.

Tags

In addition to directives, the event handler contains **tags**. Each tag represents a field if it is forwarded to BSM. 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 BSM. It can be either **INT**, **DOUBLE** or **STRING**. The default type is **STRING**.

By defining a tag, you can customize event forwarding to BSM. Thus getting more value from the external applications that create those events. For example, if the monitor pulls out data from a database table column called AlertText, which contains a textual description of an alert, it is possible to send that data to BSM 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 BSM 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 BSM. 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.

16

Integration with HP Network Node Manager

This chapter includes:

Concepts

Tasks

Concepts

Network Node Manager Integration Overview

BSM can accept events from HP Network Node Manager (NNM). 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 BSM. 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 BSM. 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 BSM.

Writing Scripts to Export Network Node Manager Data

The script you use should accept data from NNM as a command line argument, and process the data so that it can be forwarded to BSM. The following sections describe example scripts that can be used to export NNM data.

This section also includes:

➤ "Sample Script for Writing to a Log File" on page 579

➤ "Sample Script for Sending SNMP Trap Data" on page 579

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");
```

Tasks

How to Configure Events in Network Node Manager

Use the following steps to configure NNM 7.x to run a script for the requested events in NNM.

Note: For later versions of NNM and NNMi, you should consult the NNMi documentation.

---

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 box.
4. Enter the command line for the script in the **Command for Automatic Action** text box. You may use NNM variables to pass data to the command line.
5. Click **OK** to close the **Modify Events** dialog.
6. From the **File** menu in the **Event Configuration** dialog select **Save**.

Part VI

Remote Servers

17

Working with Remote Servers

This chapter includes:

Concepts

Tasks

Reference

Concepts

Remote Servers Overview

SiteScope must be able to establish a connection to the servers you want to monitor. It must also be authenticated as a user having account permissions to access the Windows performance registry on the Microsoft Windows remote machine and to run command line tools on the UNIX remote machine as a remote user.

Microsoft Windows/UNIX Remote server options are used to set up the connection properties, such as credentials and protocols, so that SiteScope can monitor systems and services running in remote environments. You can then create monitors to watch the resources and performance counters for that server. Multiple monitors can use the same connection profile. You can also create multiple remote servers for the same host machine.

Note: If multiple Windows remote servers are configured for the same host machine using the NetBIOS method, the connection fails. This is because Windows NT does not permit multiple connections to a server or shared resource by the same user, using more than one user name (System error 1219).

For details on enabling SiteScope to monitor data on remote servers, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586 and "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

For details on configuring these settings in the user interface, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603 and "New/Edit UNIX Remote Server Dialog Box" on page 610.

For information about troubleshooting and limitations of SiteScope monitoring of remote servers, see "Troubleshooting and Limitations" on page 619.

Note: You can use SiteScope UNIX operating system adapters to extend SiteScope to connect to, and remotely monitor versions of UNIX that are not supported by default. For details, see "UNIX Operating System Adapters" on page 677.

Tasks

How to Configure SiteScope to Monitor a Remote Microsoft Windows Server

This task describes the steps involved in configuring SiteScope to monitor data on remote Windows servers.

This task includes the following steps:

1 Prerequisites (for Windows Server 2008 remote servers)

SiteScope supports monitoring on Microsoft Windows Server 2008 remote servers with User Account Control (UAC) enabled or disabled. Where UAC is enabled, you must disable the UAC remote restrictions as follows:

a Click **Start**, click **Run**, type regedit, and then press ENTER.

b Locate and then click the following registry subkey: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**

c If the LocalAccountTokenFilterPolicy registry entry does not exist, follow these steps:

- On the **Edit** menu, select **New** > **DWORD Value**.
- Type **LocalAccountTokenFilterPolicy**, and then press ENTER.

d Right-click **LocalAccountTokenFilterPolicy**, and then click **Modify**.

e In the **Value data** box, type **1**, and then click **OK**.

f Exit Registry Editor.

2 Enable SiteScope to monitor data on remote Windows servers

To enable SiteScope to monitor data on remote Windows servers, you must perform one of the following steps:

- Define an individual remote Windows server connection profile for each server. For task details, see "Define Remote Windows Server Connection Profiles" on page 590.
- Set domain access privileges to permit SiteScope to access remote servers. For details on the monitor settings, see "Set Domain Privileges for SiteScope Monitoring" on page 591.

Note: If you configure the SiteScope service to run as a domain user, SiteScope uses this account for all Windows-related authorization. You must ensure that this account has the necessary privileges across the domain.

---

3 Configure user permissions for remote monitoring

Configure the user permissions to access the remote machine according to the operating system on the SiteScope machine. For details on the monitor settings, see "Configure User Permissions for Remote Monitoring" on page 593.

4 Configure and test the settings for the Windows remote server

a Configure the remote Windows server in the remote server tree. For user interface details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603.

Note:

- If you are configuring remote Windows Servers for SSH monitoring with SiteScope, see "How to Configure Remote Windows Servers for SSH monitoring" on page 647.
- If WMI is selected as the method for gathering management data from remote servers in the Main Settings **Method** field, the WMI service must be configured on the remote machine. For task details, see "Configure the WMI Service for Remote Monitoring" on page 596.
- If specifying a literal IPv6 address as the name for the remote monitored server when using the NetBIOS connection method, the IPv6 address must be customized by:

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

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

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

---

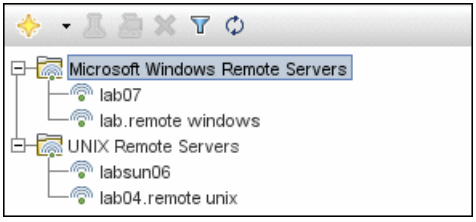
b After defining the Microsoft Windows remote server definition for SiteScope, click the **Test** button for the applicable server to test the connection.

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

---

5 Results

The server is added to the list of remote Windows Remote servers in the remote server tree. You can then create monitors to watch the resources and performance counters for that server. Multiple monitors can use the same connection profile.



Note: For information about troubleshooting and limitations of SiteScope monitoring of remote servers, see "Troubleshooting and Limitations" on page 619.

Define Remote Windows Server Connection Profiles

Monitoring remote Windows server data requires authenticated access to the remote server. A Windows server connection profile provides the necessary address and login credentials for SiteScope to log on to a remote server and to access the Windows performance registry on that remote machine.

Note: This task is part of a higher-level task. For details, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.

To log on to a remote server using the Windows server connection profile, either:

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

Set Domain Privileges for SiteScope Monitoring

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

Note: This task is part of a higher-level task. For details, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.

To set domain privileges, use one of the following methods:

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

By default, SiteScope is installed to run as a Local System account. You can set the SiteScope service to log on as a user with domain administration privileges. This gives SiteScope access privileges to monitor server data within the domain. For details on how to change the SiteScope account user, see "Change the User Account of the SiteScope Service" on page 592.

➤ **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 enable non-admin access.**

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

Change the User Account of the SiteScope Service

This task describes the steps involved in changing the user account of the SiteScope service.

Note: This task is part of a higher-level task. For details, see "Set Domain Privileges for SiteScope Monitoring" on page 591.

To change the user account of the SiteScope service:

1. In **Administrative Tools**, open **Services**, and select **SiteScope** from the list of services. The SiteScope Properties dialog box opens.
2. Click the **Log On** tab, and in the **Log on as** area, enter an account that can access the remote servers.
3. Click **OK** to save your settings and close the SiteScope Properties dialog box.
4. Right-click **SiteScope**. Click **Stop** to stop the SiteScope service.
5. Click **Start**. The SiteScope service now uses the new account.

Configure User Permissions for Remote Monitoring

For SiteScope to collect performance measurements on a remote machine, SiteScope must have permission to access the remote machine. This task describes how to configure user permissions according to the operating system on the SiteScope machine.

Note:

- This task is part of a higher-level task. For details, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.
- 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, select 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, select the user that SiteScope uses to access the remote machine. In the Permissions pane, select the **Allow** check box for **Read**. Click **OK** to save the configuration and close the Permissions for Perflib dialog box.

7 In the Registry Editor tool bar, click **Registry** and select **Exit** to save the configuration and exit.

8 Restart the SiteScope machine.

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

To configure Windows 2000:

1 On the SiteScope machine, open **Administrative Tools** and select **Computer Management**. The Computer Management dialog box opens.

2 In the System Tools tree, expand the **Local Users and Groups** tree and select **Groups**. All groups on the machine are listed in the right-hand pane.

3 In the right-hand pane, select the **Administrators** group. The Administrators Properties dialog box opens.

4. If the user that SiteScope uses to access the remote machine is listed in the Members pane, go to step 5. If the user is not listed, click **Add**. The Select Users or Groups dialog box opens.
   a. Enter the user in the text box.
   b. Click **OK** to save the configuration and close the Select Users or Groups dialog box.
5. Click **OK** to save the configuration and close the Administrators Properties dialog box.
6. In the Computer Management dialog box, click **File** in the tool bar and select **Exit**.
7. Restart SiteScope on the SiteScope machine.

Configure the WMI Service for Remote Monitoring

This task describes the steps involved in configuring SiteScope to monitor data on remote Windows servers using Windows Management Instrumentation (WMI). Using WMI, you can access system counter data from objects in the performance libraries. This is the same performance data that appears in the Perfmon utility.

Note: This task is part of a higher-level task. For details, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.

This task includes the following steps:

1 Prerequisites

SiteScope must be installed on a Windows machine.

2 Configure the WMI service on the remote server

The following are requirements for using SiteScope to collect performance measurements on a remote machine using WMI:

- The WMI service must be running on the remote machine. For details, refer to the Windows Management Instrumentation documentation (http://msdn.microsoft.com/en-us/library/aa826517(VS.85).aspx).
- The user entered on the WMI remote server must have permissions to read statistics remotely from WMI namespace **root\CIMV2**. For details, refer to http://support.microsoft.com/kb/295292.

For information about troubleshooting WMI service problems, see "WMI Troubleshooting and Limitations" on page 626.

3 Configure WMI preference settings in SiteScope - optional

You can configure the connection type for monitoring Windows server resources on the local host machine and the WMI timeout settings in **Preferences** > **General Preferences** > **WMI Preferences**. For user interface details, see "WMI Preferences" on page 703.

4 Configure a monitor

Add a WMI supported monitor, and configure the monitor settings. For the list of monitors that support the WMI protocol, see "Monitors Supporting Windows Management Instrumentation (WMI)" on page 434.

How to Configure SiteScope to Monitor a Remote UNIX Server

This task describes the steps involved in configuring SiteScope to monitor data on remote UNIX servers.

This task includes the following steps:

1 Enable SiteScope to monitor data on remote UNIX servers

To enable SiteScope to monitor data on remote UNIX servers, define an individual remote UNIX server connection profile for each server. For task details, see "Define Remote UNIX Server Connection Profiles" on page 599.

2 Configure and test the settings for the UNIX remote server

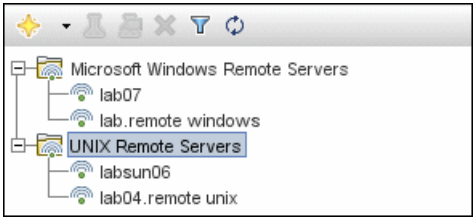
a Configure the remote UNIX server in the remote server tree. For user interface details, see "New/Edit UNIX Remote Server Dialog Box" on page 610.

b Test the settings for the applicable server.

- Click the **Test** button to test the connection to the server.
- Click the **Detailed Test** button to test the running commands on the remote host and check the permissions for the defined user.

3 Results

The server is added to the list of UNIX Remote Servers in the remote server tree. You can then create monitors to watch the resources and performance counters for that server. Multiple monitors can use the same connection profile.



Note: For information about troubleshooting and limitations of SiteScope monitoring of remote servers, see "Troubleshooting and Limitations" on page 619.

Define Remote UNIX Server Connection Profiles

Monitoring remote UNIX server data requires authenticated access to the remote server. A UNIX server connection profile provides the necessary address and login credentials for SiteScope to log on to a remote server.

Note: This task is part of a higher-level task. For details, see "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

To log on to a remote server using the UNIX server connection profile, either:

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

Reference

Remote Servers User Interface

This section includes:

Remote Server Properties Page

This page displays information about the remote servers configured in your network environment. Use this page to add, edit, or delete remote server profiles.

To access	Select the **Remote Servers** context. In the remote servers tree, click the **Microsoft Windows Remote Servers** or **UNIX Remote Servers** container.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit remote servers** permissions can view or edit the Remote Servers page. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ You cannot delete a server from the list of remote servers if the server is referenced by a monitor. Select a different server in the **Server** box of the Monitor Settings pane for each monitor that references the remote server, and then delete the remote server from the remote server list. ➤ You can create multiple remote servers for the same host machine.

Relevant tasks	➤ "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586 ➤ "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598
See also	➤ "Remote Servers Overview" on page 584 ➤ "Remote Server Tree" on page 93 ➤ "Troubleshooting and Limitations" on page 619

User interface elements are described below:

UI Element	Description
	**New Microsoft Windows/UNIX Remote Server.** Opens the New Microsoft Windows/UNIX Remote Server dialog box enabling you to configure a remote server and add it to the tree. For details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603 or "New/Edit UNIX Remote Server Dialog Box" on page 610.
	**Edit Remote Server.** Enables you to edit the properties of the selected remote server.
	**Delete Remote Server.** Deletes the selected server from the tree.
	**Test.** Tests the connection to one or multiple servers. ➤ When testing the connection to a single remote server, the test results are displayed in a popup window. ➤ When testing the connection for multiple remote servers, the test is performed in the background so you can continue to use SiteScope. The test results are displayed in **Server Statistics** > **Log Files** > **Other Logs** in the **remotes_multi_test.log**.
	**Detailed Test.** Runs a test that displays the result of running commands on UNIX remote servers. This enables checking the permissions for the defined user.
	**Select All.** Selects all listed remote servers.

UI Element	Description
	**Clear Selection.** Clears the selection.
<Remote servers list>	Lists the remote servers that have been configured in SiteScope. Double-click a remote server to open the Edit Remote Server page for the selected remote server type. For details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603 or "New/Edit UNIX Remote Server Dialog Box" on page 610.
Name	Name by which the remote server is known in SiteScope.
Server	IP address or name of the monitored remote server. You can create two remote servers with the same host name.
Status	Connection status of the remote server. If SiteScope is unable to connect to the remote server, a reason for the connection failure is provided.
Last Test	The date and time that the remote server connection was last tested.
Operating System	Operating system that is running on the remote server.
Method	Connection type for monitoring the server resources (NetBIOS, SSH, WMI, Rlogin, Telnet).
Associated Monitors	Number of monitors used by each remote server. This enables sorting the table by the number of monitors used by each remote server, and removal of unused remote servers (those with 0 associated monitors can subsequently be deleted).
Description	Description of the remote server.

New/Edit Microsoft Windows Remote Server Dialog Box

SiteScope 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	Select the **Remote Servers** context. ➤ To add a Microsoft Windows remote server, right-click the **Microsoft Windows Remote Servers** container, and select **New Microsoft Windows Remote Server**. ➤ To edit an existing Microsoft Windows remote server, expand the **Microsoft Windows Remote Servers** container, and select the remote server you want to edit.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit remote servers** permissions can view or edit the Remote Servers page. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ You cannot delete a server from the list of remote servers if the server is referenced by a monitor. Select a different server in the **Server** box of the Monitor Settings pane for each monitor that references the remote server, and then delete the remote server from the remote server list.
Relevant tasks	"How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586
See also	➤ "Remote Servers Overview" on page 584 ➤ "Remote Server Tree" on page 93 ➤ "Remote Server Properties Page" on page 600 ➤ "Troubleshooting and Limitations" on page 619

The following elements are included:

UI Element	Description
Save	Saves the settings without verifying the correctness of the configuration on the remote server. **Tip:** Performance is faster if you use **Save** instead of **Save & Test**, because SiteScope does not need to establish a connection to the remote server to verify the settings.
Save & Test	Saves the settings and verifies the correctness of the configuration on the remote server. If SiteScope fails to connect to the remote server, or if there is an invalid property in the configuration settings, an error message is displayed. **Tip:** Performance is not as fast if you use **Save & Test** instead of **Save**, because SiteScope needs to establish a connection to the remote server to verify the settings.

General Settings

User interface elements are described below:

UI Element	Description
Name	Name by which the remote machine should be known in SiteScope. This name appears in the **Server** list of monitors that can use this connection profile. **Note when working in template mode:** ➤ For each template monitor that requires this remote server, you must enter this same value in the **Servers** box for the template monitor. ➤ Names must be unique, otherwise the deployment fails.
Description	Description for the remote Windows server. This text appears only when editing the remote's properties.

Main Settings

User interface elements are described below:

UI Element	Description
Server	Real IP address or UNC name of the monitored Windows server (virtual IP addresses are not supported). An IP host name also works if the SiteScope server can translate this common name into an IP address by using a hosts file, DNS, or WINS/DNS integration. You can create multiple remote servers for the same host machine. For example, you can create one remote server that uses the NetBIOS protocol and another that uses WMI for the same host machine, provided the name in General Settings is unique. To use the same login credentials to configure multiple servers at the same time, enter the server names or addresses separated by a comma (","), semicolon (";"), or a space. For example: \\server1,\\server2,\\. **Note:** In the list of Windows Remote Servers, click the **Test** button to test connectivity after the profiles have been added. **Note when working in template mode:** Name of a template variable that represents the remote server name, for example, %%host%%. This enables you to add each server as you deploy the template when asked to enter the required information for the variables. Each time you enter a server name for the variable, a monitor instance is created for that server and the server is added to the remote server tree. If the host name does not match a server name at that time, the monitor fails. If the remote servers onto which you want to deploy monitor templates already exist under Remote Servers, you can reference these servers within the monitor template. You do this by referencing the system variable $$SERVER_LIST$$ which identifies the servers accessible to the SiteScope. For details, see "Syntax for System Variables" on page 956.

UI Element	Description
Credentials	Option for providing the user name and password for the remote Windows server: ➤ **Use user name and password.** Select this option to manually enter user credentials. ➤ **User name.** Enter the user name for the remote server or use a template variable that represents the user login name (for example, %%user%%). **Note:** 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, or use a template variable that represents the password (for example, %%password%%). When using SSH authentication with public/private key based authentication enter the passphrase for the identity file here. ➤ **Select predefined credentials.** Select this option to have SiteScope automatically supply a predefined user name and password for the server (selected by default). Select the credential profile to use from the **Credential profile** drop-down list, or click **Add Credentials** and create a new credential profile. For details on how to perform this task, see "How to Configure Credential Preferences" on page 895.
Trace	Traces messages to and from the subject server, and records them in the SiteScope **RunMonitor.log** file. **Default value:** Not selected

UI Element	Description
Method	Connection types for monitoring Windows server resources: ➤ **NetBIOS.** The default server-to-server communication protocol for Microsoft Windows NT and 2000 networks. **Note:** SiteScopes running on Windows platforms need to be running under an account that has the necessary administrative security privileges to access performance counter data from remote servers when the NetBIOS connection is used and the **Trace** option is selected. If the servers you want to monitor are in a different domain, are governed under a different policy, or require a unique login different than the account SiteScope is running under, then you must define the connection to these servers under the Microsoft Windows Remote Servers option in the remote server view. ➤ **SSH.** Secure Shell, a more secured communication protocol that can be installed on Microsoft Windows NT/2000 based networks. This connection method normally requires installing SSH libraries on each server to be connected, unless you are using agentless Windows SSH. For the list of monitors that support Windows SSH (agentless or using the SiteScope remote Windows SSH files), see "Monitors Supporting Windows SSH (Agentless or Using the SiteScope Remote Windows SSH Files)" on page 665. For more information on SSH requirements, see "SiteScope Monitoring Using Secure Shell (SSH)" on page 639. ➤ **WMI.** Windows Management Instrumentation, a more secured communication protocol than NetBIOS, supports Windows server monitors that use perfmon to gather performance data. For the list of monitors that support WMI, see "Monitors Supporting Windows Management Instrumentation (WMI)" on page 434. For details on how to configure the WMI service for remote monitoring, see "Configure the WMI Service for Remote Monitoring" on page 596. **Note:** Remote servers that have been configured with the WMI method are not displayed in the list of available remote servers when configuring a monitor that does not support WMI.

UI Element	Description
Remote server encoding	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 value:** Cp1252 encoding

Advanced Settings

User interface elements are described below:

UI Element	Description
SSH port number	Port on which the remote SSH server is listening. **Default value:** 22
Connection limit	Number of open connections that SiteScope permits 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. **Default value:** 3 **Note:** This setting does not effect running tests for a remote server. Tests always create a new connection.
SSH authentication method	Authentication method to use for SSH connections: ➤ **Password.** Authenticates using a password (default setting). ➤ **Key File.** Authenticates 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 information about SSH requirements, see "SiteScope Monitoring Using Secure Shell (SSH)" on page 639.
Disable connection caching	Turns off connection caching for this remote. By default, SiteScope caches open connections. **Default value:** Not selected

UI Element	Description
Key file for SSH connections	Path and name of 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.
SSH version 2 only	Forces SiteScope to use SSH protocol version 2 only. **Default value:** Not selected
SSH keep alive mechanism	Engages a keep alive mechanism for SSH version 2 sessions. This option applies only when using the integrated Java Client. **Default value:** Not selected
SSH using preinstalled SiteScope remote Windows SSH files	Uses preinstalled SiteScope remote Windows SSH files. For the list of monitors that support Windows SSH using SiteScope SSH files, see "Monitors Supporting Windows SSH (Agentless or Using the SiteScope Remote Windows SSH Files)" on page 665. **Default value:** Selected

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

New/Edit UNIX Remote Server Dialog Box

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	Select the **Remote Servers** context. ➤ To add a UNIX remote server, right-click the **UNIX Remote Servers** container, and select **New UNIX Remote Server**. ➤ To edit an existing UNIX remote server, expand the **UNIX Remote Servers** container, and select the remote server you want to edit.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit remote servers** permissions can view or edit the Remote Servers page. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ You cannot delete a remote server from the list of remote servers if the server is referenced by a monitor. Select a different server in the **Server** box of the Monitor Settings pane for each monitor that references the remote server, and then delete the remote server from the remote server list. ➤ The HTTP method for connecting to a remote server is no longer supported.
Relevant tasks	"How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598
See also	➤ "Remote Servers Overview" on page 584 ➤ "Remote Server Tree" on page 93 ➤ "Remote Server Properties Page" on page 600 ➤ "Troubleshooting and Limitations" on page 619

The following elements are included:

UI Element	Description
Save	Saves the settings without verifying the correctness of the configuration on the remote server. **Tip:** Performance is faster if you use **Save** instead of **Save & Test**, because SiteScope does not need to establish a connection to the remote server to verify the settings.
Save & Test	Saves the settings and verifies the correctness of the configuration on the remote server. If SiteScope fails to connect to the remote server, or if there is an invalid property in the configuration settings, an error message is displayed. **Tip:** Performance is not as fast if you use **Save & Test** instead of **Save**, because SiteScope needs to establish a connection to the remote server to verify the settings.

General Settings

User interface elements are described below:

UI Element	Description
Name	Name by which the remote machine should be known in SiteScope. This name appears in the **Server** list of monitors that can use this connection profile.
Description	Description for the remote UNIX server. This text appears only when editing the remote's properties.

Main Settings

User interface elements are described below:

UI Element	Description
Main Settings	
Server	Real IP address or host name of the monitored server (virtual IP addresses are not supported). To use the same login credentials to configure multiple servers at the same time, enter the server names or addresses separated by a comma (","), semicolon (";"), or a space. **Example:** If using NetBIOS to connect to other servers, enter a comma-separated string of server addresses such as: serveraddress1,serveraddress2,serveraddress3 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 the **Test** button in the table listing the UNIX Servers. This tests only the connection to the server. Click the **Detailed Test** button to run a test that displays the result of running commands on the remote host. This enables checking the permissions for the defined user. **Note when working in template mode:** Enter the name of a template variable that represents the remote server name, for example, %%host%%. Each time you enter a server name for the variable, a monitor instance is created for that server and the server is added to the remote server tree. If the remote servers onto which you want to deploy monitor templates already exist under Remote Servers, you can reference these servers within the monitor template. You do this by referencing the system variable $$SERVER_LIST$$ which identifies the servers accessible to the SiteScope. For details, see "Syntax for System Variables" on page 956.

UI Element	Description
Credentials	Option for providing the user name and password for the remote UNIX server: ➤ **Use user name and password.** Select this option to manually enter user credentials. ➤ **User name.** Enter the user name for the remote server or use a template variable that represents the user login name (for example, %%user%%). ➤ **Password**. Enter the password for the remote server or the passphrase for the SSH key file, or use a template variable that represents the password (for example, %%password%%). When using SSH authentication with public/private key based authentication enter the passphrase for the identity file here. ➤ **Select predefined credentials.** Select this option to have SiteScope automatically supply a predefined user name and password for the server (selected by default). Select the credential profile to use from the **Credential profile** drop-down list, or click **Add Credentials** and create a new credential profile. For details on how to perform this task, see "How to Configure Credential Preferences" on page 895.
Trace	Traces messages to and from the remote server in the **RunMonitor.log** file. **Default value:** Not selected
Operating system	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. The following operating systems are supported when defining Remote Unix servers: AIX, FreeBSD, HP-UX, HP/UX, HP/UX64-bit, Linux, MacOSX, NonStopOS, OPENSERVER, Red Hat Enterprise Linux, SCO, SGI Irix, Solaris Zones, Sun Solaris, SunOS, Tru64 5.x,and Tru64 Pre 4.x (Digital). For servers running versions of UNIX which are not included in the list, see "UNIX Operating System Adapters" on page 677.

UI Element	Description
Method	Connection types for monitoring UNIX server resources: ➤ **Rlogin.** Logs in to the remote server using the Rlogin protocol. You can set up your remote servers to require a password for rlogin, or to enable access without a password (like "rsh"). SiteScope supports either case. ➤ **SSH.** Logs in to the remote server using Secure Shell, a more secured communication protocol. This may require additional software and setup depending on the version of UNIX. For Solaris, using the SSH access method requires that an SSH client is installed on the SiteScope machine and the SSH server installed on the servers you are monitoring. The path to the SSH client on the machine where SiteScope is running should be **/usr/local/bin/ssh** or **/usr/bin/ssh**. For information about SSH requirements, see "SiteScope Monitoring Using Secure Shell (SSH)" on page 639. Using SSH requires that digital certificates be installed on each of the servers to which you are connecting. ➤ **Telnet.** Logs in to the remote server using Telnet. Telnet is a popular method for connecting to remote UNIX servers. You can set up your remote servers to require a password for telnet, or to enable access without a password (like "rsh"). SiteScope handles either case.
Prompt	Prompt output when the remote system is ready to handle a command.
Login prompt	Prompt output when the system is waiting for the login to be entered.
Password prompt	Prompt output when the system is waiting for the password to be entered.

UI Element	Description
Secondary prompt	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.
Mask secondary response	Hides the secondary response behind asterisks. If you subsequently clear the check box, the hidden data is deleted. **Default value:** Not selected
Secondary response	Responses to any secondary prompts required to establish connections with this remote server. Separate multiple responses with commas (,).

UI Element	Description
Initialize shell environment	Shell commands to be run at the beginning of the session. Separate multiple commands with a semicolon (;). This option specifies shell commands to be run on the remote machine directly after a Telnet or SSH session has been initiated. These commands can be used to customize the shell for each SiteScope remote. Some examples include: ➤ 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 run. ➤ 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 server encoding	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 value:** Cp1252 encoding

UI Element	Description
HP NonStop Shell Settings	
Shell choice prompt	(For NonStop OS only) Prompt output when the system is waiting for the shell to be selected. **Default value:** >
Shell name	(For NonStop OS only) Shell name to be executed. **Default value:** OSS

Advanced Settings

User interface elements are described below:

UI Element	Description
SSH port number	Port on which the remote SSH server is listening. **Default value:** 22
Connection limit	Number of open connections that SiteScope permits 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. **Default value:** 3 **Note:** This setting does not effect running tests for a remote server. Tests always create a new connection.
SSH authentication method	Authentication method used for SSH connections: ➤ **Password.** Authenticates using a password (default setting). ➤ **Key File.** Authenticates 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 information about SSH requirements, see "SiteScope Monitoring Using Secure Shell (SSH)" on page 639.

UI Element	Description
Disable connection caching	Turns off connection caching for this remote. By default, SiteScope caches open connections. **Default value:** Not selected
Key file for SSH connections	Path and name of 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.
SSH version 2 only	Forces SiteScope to use SSH protocol version 2 only. **Default value:** Not selected
SSK keep alive mechanism	Engages a keep alive mechanism for SSH version 2 sessions. This option applies only when using the integrated Java Client. **Default value:** Not selected

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

Troubleshooting and Limitations

This section describes troubleshooting and limitations when working with remote servers.

SiteScope Monitoring of Remote Windows Servers

The following is additional information relating to setting up and troubleshooting SiteScope monitoring of remote Windows servers.

- Connect to the remote machine using PERFMON. If a connection cannot be made using this tool, there is likely a problem involving the user access permissions granted to the SiteScope account on the remote server. SiteScope requires certain administrative permissions to be able to monitor server statistics.
- For security reasons, SiteScope may not be permitted to use the permissions of a full administrator account. SiteScope can be granted restricted monitoring access by editing certain Windows Registry Keys. For information about restricting access to the registry from a remote machine, refer to the Microsoft Knowledge Base (http://support.microsoft.com/kb/q153183/).
- When you need to monitor a server which is a standalone 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.
- If you are unable to connect to Microsoft Windows Vista or Microsoft Windows 2008 remote servers using the NetBIOS connection method, you can use the WMI connection instead.
- Some problems have been found when trying to monitor Windows 2000 servers from SiteScope running on Windows NT4. In many cases, the problem involves incompatibility of the DLL's used by the operating system to communicate between the servers.

Note:

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

Recommended Network Settings for Monitoring Windows Servers

When monitoring Windows-based servers, it is recommended to disable NetBios over TCP/IP on networks where WINS in not enabled to avoid network-related errors such as "System error: 53 - The network path was not found".

1. Open **Network Connections**.
2. Right-click the network connection you want to configure, and then click **Properties**.
3. On the **General** tab, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. Click **Advanced**, click the **WINS** tab, and then select the **Disable NetBios over TCP/IP** option.

Understanding Error Codes When Testing Windows Remote Servers

Problem:

In the remote server test results, the status string does not contain descriptive error codes.

Resolution:

Use the net helpmsg command to help explain Windows network messages and provide problem-solving information.

Run the following command line:

```
net helpmsg <error code number>
```

For example, entering net helpmsg 53 returns "The network path was not found."

Microsoft Windows Event Log Access on Remote Windows Servers

Problem:

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

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

Cause:

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

Resolution:

The required registry entries and DLL files must be copied to the remote computer on which the event viewer application is being run.

To get the remote registry entries and DLL files onto the local SiteScope machine:

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

```
Source: 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 must update the registry in step 3 to reflect the directory in which the DLL is located.

SiteScope Uses the Wrong Credentials for Remote Windows Connections Using Perfex

Problem:

SiteScope ignores the credentials provided for specific remotes and tries to run monitoring commands and actions for perfex-based monitors (such as CPU, Memory, and Windows monitors) using credentials that are used to start the SiteScope service.

Resolution:

For perfex-based monitors to work correctly with remote servers, you must add the **_perfexOptions=-optionalSetupConnection** property to the **master.config** file in the **<SiteScope root directory>\groups** folder.

Viewing Data Returned when SiteScope is Trying to Access the Remote Registry

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

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

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

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

```
DEBUG: perfex debugging on

mode: elast
LOGNAME: Application
RECORD: 0
MACHINE: \\g11
Connected to \\g11 as g11nadmin
OLDEST RECORD=1
NUMBER OF RECORDS=2078
Next Record: 2079
```

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.
```

WMI Troubleshooting and Limitations

WMI Limitations

- It is not recommended to have more than 4000 monitors using WMI.
- When a counter or object is shared between resources, SiteScope is unable to receive data for the counters and the query fails. If other counters are referenced in the same query, they also fail to receive data. For details and troubleshooting information, refer to http://support.microsoft.com/kb/836802.

WMI Fails to Retrieve Counters

In some cases, WMI shows n/a for counters while perfmon gives the value 0 for the same counters. This is the behavior for counters that are also not selectable using the perfmon utility. The reason that perfex can get values for these counters is because it bypasses perfmon and accesses them through the registry.

WMI Data Not Synchronized

WMI data relies on being synchronized with the Perfmon utility. If WMI data is not synchronized, you should perform the following:

1. Check that the WMI service is started on the target machine. For details, refer to http://msdn.microsoft.com/en-us/library/aa826517(VS.85).aspx.
2. Check that the namespace **root\CIMV2** is configured to enable remote access to the user specified in the SiteScope WMI remote server. For details, refer to http://support.microsoft.com/kb/295292.
3. On the target machine, run the command **perfmon** and verify that the required perfmon objects appear. For details, refer to http://msdn.microsoft.com/en-us/library/aa645516(VS.71).aspx.

   For details on how to rebuild these libraries, refer to http://support.microsoft.com/?kbid=300956.
4. On the target machine, run the command **perfmon /wmi** and verify that the required perfmon objects appear. For details, refer to http://msdn.microsoft.com/en-us/library/aa645516(VS.71).aspx.

   If the required perfmon objects do not appear, run the command **perfmon wmiadap /f**. For details, refer to http://msdn.microsoft.com/en-us/library/aa394528(VS.85).aspx.

Remote UNIX Servers Not Configured for an English Locale

Problem:

The File Monitor and Directory Monitor may fail when using UNIX remote servers that are not configured by default for an English locale or language.

Resolution:

Add "LANG=C; export LANG" to the **Initialize shell environment** property of the problematic UNIX remote server.

System Encoding Used When Displaying System Resources for Remote Hosts Connected Through NETBIOS

This limitation affects all server monitors that use encoding of the remote host to display received data.

SiteScope uses default system encoding when displaying system resources information for the remote hosts connected through NETBIOS. The **Remote server encoding** field (available in the remote server's "Main Settings" on page 605) is not used. For example, if system encoding is ASCII and remote encoding is Unicode, the ASCII characters are displayed correctly and the Unicode symbols are not supported.

18

IP Version 6 Support in SiteScope

This chapter includes:

Concepts

Tasks

Reference

Concepts

Support for IP Version 6

Internet Protocol version 6 (IPv6) is a new version of the Internet Protocol for the Network layer of the Internet. IPv6 is designed to solve many of the problems of the current version of IP (known as IPv4) such as address depletion, security, autoconfiguration, and extensibility.

The level of support for IPv6 depends on the operating system on which SiteScope is installed. Windows Server 2008 has full-featured support for IPv6, which is installed and enabled by default. As a result, IPv6 is supported by most SiteScope monitors when SiteScope is installed on Windows Server 2008 and later. Support for IPv6 on Windows Server 2003 is limited, as many core services and networking components do not support it. IPv6 is also fully supported when SiteScope is installed on UNIX operating systems that provide full support for IPv6.

By default, SiteScope connects to remote servers using IPv4 addresses. If you want your environment to resolve host names to IPv6, you can select the **Prefer IP version 6 addresses** option in SiteScope Infrastructure Settings. When this option is selected, the following must occur for the IPv6 over IPv4 preference to take effect:

- A host name must be specified for the remote server. If an IP address is specified, the prefer IPv6 setting has no effect on the host since the IP address determines the IP version that is used.
- The host name resolves to both an IPv4 and an IPv6 address. If the host name resolves only to an IPv4 address, then the IPv4 address is used.

Note:

- If a host name is specified and the host name resolves to both an IPv4 and an IPv6 address, but the monitor does not support IPv6, the monitor will not work. For details on how to resolve this issue, see "Working in a Mixed IPv4 and IPv6 Environment" on page 632. For the list of monitors supporting IPv6, see "Monitors Supporting IP Version 6 Addresses" on page 636.
- When specifying a literal IPv6 address as the name for the remote monitored server when using the NetBIOS connection method, the IPv6 address must be customized by:

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

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

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

This section also includes:

Working in a Mixed IPv4 and IPv6 Environment

When working in a mixed environment where both IPv4 and IPv6 are used, the DNS server might return both an IPv4 and an IPv6 address for a host name. To instruct SiteScope which IP address to use for each resolved host name, you can:

- Select the **Prefer IP version 6 addresses** option, and perform one of the following (for the hosts that you want to use the IPv4 protocol):
  - Enter the IP address instead of the host name for the specified remote server.
  - Configure the DNS server so that the host name resolves to the IP address that you want to use for the remote server. You can do this by removing the IPv6 address from the DNS server for the specified host.
- Clear the **Prefer IP version 6 addresses** option, and perform the following (for the hosts that you want to use the IPv6 protocol):
  - Enter the IP address instead of the host name for the specified remote servers.
  - Configure the DNS server so that the host name resolves to the IP address that you want to use for the specified remote servers. You can do this by removing the IPv4 address from the DNS server for the specified hosts.

For details on enabling IPv6 addressing in SiteScope, see "How to Enable SiteScope to Prefer IP Version 6 Addresses" on page 634.

Supported Protocols

The following protocols are supported when IPv6 is used in SiteScopes installed on Windows and UNIX platforms:

Target	SiteScope Installed on Windows Platform	SiteScope Installed on UNIX Platform
Windows	NetBios WMI	SSH
UNIX	Not supported	SSH

Note:

- SiteScope installed on Windows platforms can monitor Windows machines only.
- NetBIOS and WMI are only supported when SiteScope is installed on Windows. SSH is not supported on Windows.
- SSH is supported only when SiteScope is installed on UNIX machines. For the list of Windows-based monitors that are supported in SiteScopes running on UNIX using SSH, see "Monitors Supporting Windows SSH (Agentless or Using the SiteScope Remote Windows SSH Files)" on page 665.

Tasks

How to Enable SiteScope to Prefer IP Version 6 Addresses

This task describes how to enable SiteScope to prefer IPv6 addresses over IPv4 when connecting to remote servers.

This task includes the following steps:

- "Enable SiteScope to prefer IPv6 addresses" on page 634
- "Customize IPv6 address as the name for the remote monitored server (for specific monitors only)" on page 635

1 Enable SiteScope to prefer IPv6 addresses

In **Preferences** > **Infrastructure Preferences** > **Server Settings**, select **Prefer IP version 6 addresses**.

For user interface details, see "Server Settings" on page 717.

Note:

- You must restart SiteScope before changes to this setting can take effect.
- If a host name is specified and the host name resolves to both an IPv4 and an IPv6 address, but the monitor does not support IPv6, the monitor will not work. For details on how to resolve this, see "Working in a Mixed IPv4 and IPv6 Environment" on page 632.

---

2 Customize IPv6 address as the name for the remote monitored server (for specific monitors only)

Some monitors have additional customization requirements or limitations when using IPv6 addressing.

For monitors that require additional IPv6 address customization, see "Monitors Supporting IP Version 6 Addresses" on page 636.

Reference

Monitors Supporting IP Version 6 Addresses

The following lists the monitors that support IPv6. Monitors that require additional IPv6 address customization in SiteScopes are indicated by an asterisk (*).

- *Citrix Monitor
- *ColdFusion Server Monitor
- *CPU Monitor
- Database Counter Monitor
- Database Query Monitor
- DB2 8.x and 9.x Monitor
- Disk Space Monitor
- *Log File Monitor
- *Memory Monitor
- *Microsoft A/V Conferencing
- *Microsoft Archiving Server
- *Microsoft ASP Server Monitor
- *Microsoft Director Server
- *Microsoft Edge Server
- *Microsoft Front End Server
- *Microsoft IIS Server Monitor
- *Microsoft Mediation Server
- *Microsoft Monitoring and CDR Server
- *Microsoft Registrar Server
- *Microsoft SQL Server Monitor

- *Microsoft Windows Event Log Monitor
- *Microsoft Windows Resources Monitor
- *Microsoft Windows Media Server Monitor
- Oracle Database Monitor
- Ping Monitor
- Port Monitor
- *Real Media Server Monitor
- *Service Monitor
- UNIX Resources Monitor
- *URL Monitor
- *URL Content Monitor
- *URL List Monitor
- *URL Sequence Monitor
- *Web Service Monitor

19

SiteScope Monitoring Using Secure Shell (SSH)

This chapter includes:

Concepts

Tasks

Reference

Concepts

SiteScope and SSH Overview

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.

Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely accessing a remote computer. It is widely used by network administrators to remotely control Web and other kinds of servers. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by encryption. Secure Shell client machines make requests of SSH daemons or servers on remote machines.

Monitoring with SiteScope over SSH has the following basic requirements:

1. The servers that you want to have monitored by SiteScope using SSH must have a SSH daemon (or server) installed and active.
2. The SiteScope integrated Java SSH client. SiteScope includes a SSH client written in Java and native to the SiteScope application code.

This section also includes:

➤ "SSH Connectivity Options" on page 641

➤ "Guidelines" on page 643

SSH Connectivity Options

The following tables outline the SSH connectivity options currently supported with SiteScope. For important information about configuring and managing SSH connectivity, see "Guidelines" on page 643.

SiteScope Installed on Windows Platform:

Target	SiteScope Client Options	Relevant Target Servers	Comments
Windows	SiteScope integrated Java SSH Client	SSH server (Cygwin OpenSSH)	➤ Agentless SSH. The RemoteNTSSH package is not required for monitors that support agentless SSH. For a list of agentless SSH supported monitors, see "Monitors Supporting Windows SSH (Agentless or Using the SiteScope Remote Windows SSH Files)" on page 665. ➤ SSH using the SiteScope remote Windows SSH files. The RemoteNTSSH package should be installed under the home user directory on the remote server. For details, see "Install SiteScope Remote Windows SSH Files" on page 661.
UNIX/ Linux	SiteScope integrated Java SSH Client	SSH host daemon (**sshd** - either proprietary or OpenSSH)	

SiteScope Installed on UNIX or Linux Platform:

Target	SiteScope Client Options	Relevant Target Servers	Comments
Windows	➤ SiteScope integrated Java SSH Client ➤ SSH client (/usr/local/bin/ssh or usr/bin/ssh)	SSH server (Cygwin OpenSSH)	➤ Agentless SSH. The RemoteNTSSH package is not required for monitors that support agentless SSH. For a list of agentless SSH supported monitors, see "Monitors Supporting Windows SSH (Agentless or Using the SiteScope Remote Windows SSH Files)" on page 665. ➤ SSH using the SiteScope remote Windows SSH files. The RemoteNTSSH package should be installed under the home user directory on the remote server. For details, see "Install SiteScope Remote Windows SSH Files" on page 661.
UNIX/ Linux	➤ SiteScope integrated Java SSH Client ➤ SSH client (/usr/local/bin/ssh or usr/bin/ssh)	SSH host daemon (**sshd** - either proprietary or OpenSSH)	

Guidelines

➤ There are two different versions of the SSH protocol: version 1 and version 2. Version 1 and version 2 are different protocols and are not compatible with each other. This means that the SSH clients and SSH hosts must be configured to use the same protocol version between them to communicate. In many cases, SSH version 1 (SSH1) is the default version used. Some security vulnerabilities have been found in SSH version 1. Also, the SSH1 protocol is not being developed anymore and SSH2 is considered the current standard.

Tip: 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.

Monitoring Remote Windows Servers Using SSH

The default remote connection method used by SiteScope for Windows-to-Windows connectivity and monitoring in Windows NT/2000/2003 networks is NetBIOS. While this has provided ease of connectivity, it does have several disadvantages. One is that NetBIOS is relatively vulnerable in terms of network security. Another is that it does not support remote execution scripts. Running commands on remote servers requires that scripts be run locally with commands to the remote machine being written using the UNC syntax of remote servers. Even then, some parameters are not returned from the remote server by using NetBIOS.

Note: SiteScope also supports the Windows Management Instrumentation (WMI) protocol which is a more secured communication protocol than NetBIOS for gathering data from remote servers running on Windows servers. For details on configuring the WMI service on the remote machine, see "Configure the WMI Service for Remote Monitoring" on page 596.

SiteScope supports monitoring of remote Windows NT/2000 servers using SSH. This technology has been tested with the OpenSSH binaries from Cygwin (available at http://www.cygwin.com/) installed as the SSH server on the remote server. It has also been tested with the server available from F-Secure. You can also try OpenSSH for Windows (formerly Network Simplicity "OpenSSH on Windows") which is available on SourceForge (available at http://sshwindows.sourceforge.net/).

The following is a comparison overview of two of the packages.

OpenSSH Package	Advantages	Disadvantage
Cygwin OpenSSH	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.
- If there is more than one version of the Cygwin utilities or more than one SSH server installed on a machine, there may be conflicts that prevent the SSH connections from working. An error message such as could not find entry point is one indication of this kind of conflict. If you suspect this error, search the machine for multiple copies of cygwin1.dll. It may be necessary to remove all versions of the utilities and then reinstall only a single installation to resolve this problem.

For details on configuring remote Windows servers for SSH monitoring, see "How to Configure Remote Windows Servers for SSH monitoring" on page 647.

Tasks

How to Configure Remote UNIX Servers for SSH monitoring

SiteScope for Solaris or Linux supports remote monitoring by using SSH. This task describes the steps involved in configuring remote UNIX Servers for SSH monitoring with SiteScope.

Note: Setting up the SSH hosts on the remote servers you want to monitor in the UNIX environment can be very complex and is beyond the scope of this document. Some suggested resources on installation of the OpenSSH daemon are http://www.sunfreeware.com/openssh.html (for Solaris) and http://docs.redhat.com/docs/en-US/Red_Hat_Network_Satellite/5.4/html/Reference_Guide/s1-mon-rhnmd.html (for Redhat Linux).

This task includes the following steps:

- "Prerequisites" on page 647
- "Configure the SSH client to connect to the remote servers" on page 647
- "Configure UNIX remote settings to use the SSH connection method" on page 647

1 Prerequisites

For details on the requirements for configuring remote UNIX servers for SSH monitoring with SiteScope in a UNIX environment, see "SSH Configuration Requirements For UNIX Remote Servers" on page 664.

2 Configure the SSH client to connect to the remote servers

After you have set up SSH servers or daemons on remote servers, you must configure the integrated Java SSH client that SiteScope uses to connect to the remote servers.

For task details, see "How to Configure the Integrated Java SSH Client" on page 673.

3 Configure UNIX remote settings to use the SSH connection method

Once you have confirmed SSH connectivity, create or configure UNIX remote settings in SiteScope to use SSH as the connection method.

For user interface details, see "New/Edit UNIX Remote Server Dialog Box" on page 610.

How to Configure Remote Windows Servers for SSH monitoring

This task describes the steps involved in configuring remote Windows Servers for SSH monitoring with SiteScope.

This task includes the following steps:

- "Install and configure a SSH server" on page 648
- "Enable Windows SSH monitoring using preinstalled SiteScope SSH files - optional" on page 648
- "Configure the SSH client to connect to the remote servers" on page 649
- "Configure Windows remote settings to use the SSH connection method" on page 649

1 Install and configure a SSH server

Install and configure a SSH server on each remote server to which you want SiteScope to connect. There are two software packages generally available that enable SSH capability:

- Cygwin environment available from http://www.cygwin.com/. For task details, see "Install Cygwin OpenSSH on Windows" on page 650.
- OpenSSH for Windows available at OpenSSH for Windows. For task details, see "Install OpenSSH for Windows" on page 658.

Note: These setup steps must be performed for each server that runs the SSH daemon or server.

---

2 Enable Windows SSH monitoring using preinstalled SiteScope SSH files - optional

Depending on the monitor that you are using, you can choose to use preinstalled SiteScope SSH files or agentless Windows SSH for monitoring the remote server (for the list of supported monitors, see "Monitors Supporting Windows SSH (Agentless or Using the SiteScope Remote Windows SSH Files)" on page 665).

- **Using preinstalled SiteScope remote Windows SSH files**. To enable SSH monitoring of the remote server using the preinstalled SSH files, you must install the SiteScope remote Windows SSH files on each remote server to enable commonly used server monitoring functions. For task details, see "Install SiteScope Remote Windows SSH Files" on page 661.
- **Agentless SSH**. If you are using agentless Windows SSH, you do not need to install SiteScope remote Windows SSH files on the remote Windows server.

Tip: If a monitor supports both preinstalled SiteScope SSH files and agentless Windows SSH, we recommend using agentless Windows SSH.

---

3 Configure the SSH client to connect to the remote servers

After you have set up SSH servers or daemons on remote servers, you must configure the integrated Java SSH client that SiteScope uses to connect to the remote servers. For task details, see "How to Configure the Integrated Java SSH Client" on page 673.

4 Configure Windows remote settings to use the SSH connection method

After confirming SSH connectivity between SiteScope and the remote server, set up Windows remote server settings in SiteScope as follows:

- In Main Settings, select **SSH** as the connection method. You can then configure monitors to use the SSH connectivity.
- To enable SSH monitoring of the remote server using the preinstalled SiteScope SSH files, make sure **SSH using preinstalled SiteScope remote Windows SSH files** is selected in the Advanced Settings pane (this is the default setting).
- To monitor using agentless Windows SSH, clear the **SSH using preinstalled SiteScope remote Windows SSH files** check box in the Advanced Settings pane.

  For user interface details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603.

Install Cygwin OpenSSH on Windows

This task describes the steps involved in installing and configuring a Cygwin OpenSSH server on Windows servers.

Note:

- This task is part of a higher-level task. For details, see "How to Configure Remote Windows Servers for SSH monitoring" on page 647.
- The following instructions assume that no other Cygwin or other ssh utilities are installed on the machine and that the machine has Internet access.
- The user login account used to install and run the SSH daemon needs adequate permissions to install the necessary programs, configure several file options, and control Windows services. It does not need to be the account that SiteScope uses to connect to the subject server, although that account must be configured within the Cygwin installation before you can monitor that server with SiteScope.

To install and configure a Cygwin OpenSSH server on Windows NT/2000 servers:

1. Create a new System Environment variable with the following definition: CYGWIN = ntsec tty.
2. Add the string ;C:\cygwin\bin to your PATH variable. Save the changes to the variables.
3. Download the Cygwin setup program into a temporary folder. For example: C:\temp. The setup program is used to select, download, and install different packages and components available with Cygwin.
4. Run the downloaded setup program and choose the **Install from Internet** option when prompted to Choose A Download Source. Click **Next** to continue.
5. If prompted, select a root install directory where the Cygwin package should be installed. This is where the SSH daemon and related files are installed. For example, C:\cygwin. Click **Next** to continue.

6 If prompted, select a temporary directory where the Cygwin installation files should be stored. For example, C:\temp. Click **Next** to continue.

7 If prompted, select an Internet Connection option. Normally, **Direct Connection** can be used. Click **Next** to continue.

8 Select a suitable mirror site from which to retrieve the files using the selection list when prompted. Click **Next** to continue.

9 The Setup program queries the mirror site for the packages available and displays a hierarchy tree of package categories. To view and select the packages to download, click on the plus (+) symbol to the left of the category name to expand any of the package trees. Packages that are selected for download and installation display a version number in the **New** column. If a version number is not displayed for a particular package, it is not downloaded and installed. Click **Skip** to the left of package name to select the package for download.

Note: Many of the development (Devel) and database (Database) tools that may be selected by default for download are not necessary to run the SSH daemon and can be deselected to reduce download time and installation space.

Select each of the following packages for download and installation:

- cygrunsrv from the Admin branch
- cygwin-doc from the Doc branch
- pdksh from the Shells branch
- openssh and openssl from the Net branch
- your choice of UNIX-style text editor from the Editors branch (for example: vim or emacs)

Then click to download the files as prompted.

10 Depending on your installation options, the Cygwin setup downloads and installs the selected packages. You may be prompted to choose to have a shortcut to the Cygwin terminal window added to the Desktop or Program Start menu. Click to continue and complete the installation.

11 After the Cygwin setup is complete, open a Cygwin terminal window by clicking on the **Cygwin** desktop shortcut or Program Start menu item.

Note: Depending on the user profile in the Windows system, the default directory that opens in the terminal window may not be within the root Cygwin installation tree. Use the `pwd` command to display the current directory. Typing in the command string `cd /` normally changes the directory to the Cygwin root, which by default corresponds to the Windows `C:\cygwin` directory.

Update the default Cygwin group file with the group names in use on the machine and on your network. Use the mkgroup utility to update the default Cygwin group file with the groups defined on the server and in your domain. Examples of the commands to use are as follows:

```
mkgroup -l >> ../etc/group
mkgroup -d >> ../etc/group
```

Note:

- To have Cygwin recognize both domain and local group accounts, run the mkgroup utility twice, once for local users (-l option) and once for domain users (-d option). Remember to use >> syntax and not just >, to append entries to the file.
- If you use both the local and domain options, you must manually edit the /etc/group file (using the UNIX style text editor you downloaded) to remove any duplicate group entries. You may also want to remove group entries that are not needed for monitoring or should not have access to this machine.

Update the default Cygwin user (passwd) file with the users defined on the local machine plus any individual domain users you want to grant access to Cygwin on this machine. Use the mkpasswd utility to update the default Cygwin user file.

Examples of the commands to use are as follows:

```
mkpasswd -l >> ..\etc\passwd
mkpasswd -d -u username >> ..\etc\passwd (domain users)
```

Note:

- By default, Cygwin is set to run the OpenSSH daemon as the local user called SYSTEM. To have Cygwin recognize both domain and local machine user accounts, run the mkpasswd using the -l option to add all local users, and run it with the -d and -u options to add individual domain users. Remember to use >> syntax and not just >, to append entries to the file.
- If you use both the local and domain options, you must manually edit the /etc/passwd file (using the UNIX style text editor you downloaded) to remove any duplicate user entries. You may also change the default /home path and default shell for individual users. This may be necessary to install the RemoteNTSSH package in the /home/sitescopeaccount/ directory of the user account to be used by SiteScope.

---

12 Change the active directory to the /bin directory by typing cd /bin.

13 Create a symbolic link in the /bin directory that points to the Windows Command (CMD) shell by entering the following command line (be sure to include the trailing space and period):

```
ln -s /cygdrive/c/winnt/system32/cmd.exe .
```

14 We recommend that you change permissions and ownership of several Cygwin files and directories. Also create a log file for the SSH daemon. Enter the following command lines in the Cygwin terminal command line and press ENTER after each command line entered:

```
cd /
chmod -R og-w .
chmod og+w /tmp
touch /var/log/sshd.log
```

Note:

- Exact syntax is required, including spaces.
- Inconsistent and incorrectly assigned file and directory permissions can be one reason that the SSH daemon can not be started or that SiteScope is unable to connect to and run commands or scripts on the remote server.

---

15 Configure the SSH daemon to run as a Windows service by entering the following command:

```
ssh-host-config -y
```

When presented with the CYGWIN= prompt, type ntsec tty to match the environment variable you set at the beginning of this procedure. Normally, this configures the SSH daemon or service to restart automatically if the server needs to be restarted.

16 Configure the encryption keys and files for the SSH daemon using the following command:

```
ssh-user-config -y.
```

Enter required passphrases for several keystore files when prompted. The program asks you to re-enter the passphrase for confirmation.

17 You must change the ownership of several files and folders for use by the SSH daemon. The program does not normally run if the permissions on these files enable them to be changed or run by group or "world" level users. Enter the following command strings to restrict access to these files:

```
chown SYSTEM:Users /var/log/sshd.log /var/empty /etc/ssh_h*
chmod 755 /var/empty
```

18 Check the installation by starting and then stopping the CYGWIN sshd service using the **Programs** -> **Administrative Tools** -> **Services** panel.

Note: Cygwin includes a server utility to start the SSH daemon. However, there have been a number of situations where this method failed to start the server, whereas using the Windows Services panel was able to start the server.

---

19 Configure the default shell or command environment for the user account you use for monitoring with SiteScope. The shell you select effects what types of scripts or commands can be run remotely using the SSH connection. Use the UNIX-style text editor and edit the **/etc/passwd** file. Find the entry for the SiteScope login account you intend to use and change the shell from **/bin/bash** to the shell you want to use as described below. This is normally the last entry in the line for that account entry.

- 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.
- If you chose to have SiteScope interact with the remote Windows server using a Cygwin UNIX shell, change the default shell entry to be **/bin/pdksh**. The SiteScope SSH client may not accurately parse Cygwin's default **bash** shell. You must also configure a Remote UNIX server connection to this (Windows) server that connects to the Cygwin SSH daemon.

Save the changes to the file.

20 Edit the PATH and the default prompt commands in the /etc/profile file to make sure that Cygwin can find certain files and that SiteScope can parse the output from the remote shell. Use the UNIX-style text editor and edit the /etc/profile file. Find the PATH definition entry near the top of the file. For example:

```
PATH=/usr/local/bin:/usr/bin:/bin:$PATH
```

Change this to include the following:

```
PATH=.:/usr/local/bin:/usr/bin:/bin:$PATH
```

21 To change the default prompt commands, edit the /etc/profile file, and find the section similar to the following:

```
;;
sh  | -sh   | */sh  |\
sh.exe  | -sh.exe   | */sh.exe )
#Set a simple prompt
PS1='$ '
;;
```

Immediately under this entry, add the following:

```
;;
pdksh  | -pdksh   | */pdksh  |\
pdksh.exe  | -pdksh.exe   | */pdksh.exe )
#Set a simple prompt
PS1='> '
;;
```

22 Save the changes to the file.

23 Change the active directory to the home directory of the user you have created for SiteScope monitoring.

After making these changes and starting the SSH daemon, you should be able to connect to the server using an SSH client.

Note: Any time you run the mkpasswd -l /etc/passwd command (for example, when adding a new user), edit the /etc/passwd file again to make sure that the default shell for that user is set to the required value for any account being used by SiteScope.

Install OpenSSH for Windows

This task describes the steps involved in installing and configuring an OpenSSH server on Windows servers.

The OpenSSH for Windows package is an alternative to the Cygwin SSH package and can be easier to install. Like most products, the Cygwin product and the Open SSH for Windows are subject to change. There are cases where some versions of the Cygwin SSH server have not returned the data needed for SiteScope monitoring. If the OpenSSH for Windows package can solve this problem, you should use this package in place of the Cygwin package.

Note: This task is part of a higher-level task. For details, see "How to Configure Remote Windows Servers for SSH monitoring" on page 647.

To install and configure an OpenSSH for Windows server on Windows NT/2000 servers:

1. Download and install the OpenSSH for Windows package.
2. Open a command prompt and change to the installation directory (C:\Program Files\OpenSSH is the default installation path).
3. Change the active directory to the OpenSSH\bin directory.

4 You must update the default group file with the group names in use on the machine and in your network. Use the mkgroup utility to update the default OpenSSH group file with the groups defined on the server and in your domain. Examples of the commands to use are as follows:

```
mkgroup -l >> ..\etc\group
mkgroup -d >> ..\etc\group
```

Note:

- To have OpenSSH recognize both domain and local group accounts, run the **mkgroup** utility twice, once for local users (-l option) and once for domain users (-d option). Remember to use >> syntax and not just >, to append entries to the file.
- If you use both the local and domain options, you must manually edit the /etc/group file (using the UNIX style text editor you downloaded) to remove any duplicate group entries. You may also want to remove group entries that are not needed or should not have access to this machine.

---

5 You must update the default OpenSSH user (passwd) file with the users defined on the local machine plus any domain user you want to grant access to the SSH server on this machine. Use the **mkpasswd** utility to update the default user file. Examples of the commands to use are as follows:

```
mkpasswd -l >> ..\etc\passwd
mkpasswd -d -u username >> ..\etc\passwd
```

Note:

- To have OpenSSH recognize both domain and local machine user accounts, run the **mkpasswd** utility using the -l option to add all local users and run it with the -d and -u options to add individual domain users. Remember to use >> syntax and not just >, to append entries to the file.
- If you use both the local and domain options, you must manually edit the /etc/passwd file (using the UNIX style text editor you downloaded) to remove any duplicate user entries. You may also change the default /home path and shell for individual users (see instructions below).

---

6 Check the installation by starting the **OpenSSH Server** service using the **Programs** > **Administrative Tools** > **Services** panel.

Install SiteScope Remote Windows SSH Files

This task describes the steps involved in installing SiteScope remote Windows files on each remote Windows server according to the SSH package you are working with.

Note:

- This task is part of a higher-level task. For details, "How to Configure Remote Windows Servers for SSH monitoring" on page 647.
- SiteScope remote Windows files do not need to be installed on remote Windows server monitors that support agentless SSH. For a list of monitors that support agentless SSH, see "Monitors Supporting Windows SSH (Agentless or Using the SiteScope Remote Windows SSH Files)" on page 665.

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 enables SiteScope to run scripts on the remote server running the SSH daemon. To be able to use the Script Monitor to run remote scripts, create a **scripts** subdirectory in the **/home/sitescope_login_account_name** directory. Scripts you create for execution by the SiteScope Script Monitor must be placed inside this directory.
3. On the machine where SiteScope is installed, find the file called **RemoteNTSSH.zip** in the **<SiteScope root directory>\tools** directory.

4 Copy this file to the **<install_drive>:\cygwin\home\sitescope_login_account_name** directory on each of the remote Windows NT/2000 servers where you have installed the SSH server or daemon software.

5 Unzip the **RemoteNTSSH.zip** file on the remote server. Place the contents of the zip file into the **<install_drive>:\cygwin\home\sitescope_login_account_name** directory. This should create a **<install_drive>:\cygwin\home\sitescope_login_account_name\scripts** subfolder. You use this subfolder to hold scripts that can be run by the SiteScope Script Monitor.

Note: If the **RemoteNTSSH.zip** file is from a version of SiteScope earlier than 11.10, you must reinstall the zip file from **<SiteScope 11.10 root>\tools** directory on all monitored remote servers.

---

6 Start the CYGWIN sshd service on the remote server.

To install the SiteScope SSH Files on OpenSSH for Windows installations:

1 On the machine where SiteScope is installed, find the file called **RemoteNTSSH.zip** in the **<SiteScope root directory>\tools** directory.

2 Copy this file to the user home directory where the user is automatically directed after logging on to the machine using the SSH server that was previously installed. This is the directory on each of the remote Windows NT/2000 servers where you have installed the SSH server or daemon software.

3 Unzip the **RemoteNTSSH.zip** file on the remote server into the user home directory. This should create a **<user home directory>\scripts** subfolder. You use this subfolder to hold scripts that can be run by the SiteScope Script Monitor.

Note: If the **RemoteNTSSH.zip** file is from a version of SiteScope earlier than 11.10, you must reinstall the zip file from **<SiteScope 11.10 root>\tools** directory on all monitored remote servers.

---

4 Start the OpenSSH server service on the remote server.

Reference

SSH Configuration Requirements For UNIX Remote Servers

The following are requirements for configuring remote UNIX servers for SSH monitoring with SiteScope in a UNIX environment:

- Secure Shell daemons or servers (sshd) must be installed on each remote server you want to monitor with SiteScope.
- The SSH daemons on the remote servers must be running and the applicable communication ports must be open. For example, the default for SSH is port number 22.
- A SSH client must be installed on the server where SiteScope is running. The SiteScope integrated Java SSH client fills this requirement.

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.

Once you have confirmed SSH connectivity, create or configure UNIX Remote settings in SiteScope to use SSH as the connection method.

Monitors Supporting Windows SSH (Agentless or Using the SiteScope Remote Windows SSH Files)

The following lists the monitors that support agentless Windows SSH, or Windows SSH using the SiteScope's remote Windows SSH files. All the monitors that support Windows SSH using SiteScope's SSH files are supported in SiteScopes running on UNIX platforms.

Monitor	Supports Windows SSH Using SiteScope's Remote Windows SSH Files	Supports Agentless Windows SSH
Citrix Monitor	✔	✔
ColdFusion Server Monitor	✔	✔
CPU Monitor	✔	✔
Directory Monitor	✔	
Disk Space Monitor	✔	✔
Log File Monitor	✔	
Memory Monitor	✔	✔
Microsoft Archiving Server Monitor	✔	✔
Microsoft A/V Conferencing Server Monitor	✔	✔
Microsoft ASP Server Monitor	✔	✔
Microsoft Director Server Monitor	✔	✔
Microsoft Edge Server Monitor	✔	✔
Microsoft Front End Server Monitor	✔	✔
Microsoft Hyper-V Monitor	✔	✔
Microsoft IIS Server Monitor	✔	✔
Microsoft Mediation Server Monitor	✔	✔

Monitor	Supports Windows SSH Using SiteScope's Remote Windows SSH Files	Supports Agentless Windows SSH
Microsoft Monitoring and CDR Server Monitor	✔	✔
Microsoft Registrar Server Monitor	✔	✔
Microsoft SQL Server Monitor	✔	✔
Microsoft Windows Event Log Monitor	✔	
Microsoft Windows Media Server Monitor	✔	✔
Microsoft Windows Performance Counter Monitor	✔	
Microsoft Windows Resources Monitor	✔	✔
Microsoft Windows Services State Monitor	✔	
Real Media Server Monitor	✔	✔
Script Monitor	✔	
Service Monitor	✔	

Troubleshooting and Limitations

This section contains troubleshooting and limitations when monitoring using SSH.

Skips in Windows SSH Based Monitors on Linux RedHat 5

If you encounter skips in Windows SSH based monitors running on Linux RedHat 5 platforms, in the **opt/SiteScope/java/lib/security/java.security** file, you should change:

“securerandom.source=file:/ dev/urandom” to

“securerandom.source=file:///dev/urandom”

Agentless Windows SSH is Not Working

If Windows SSH is working using the SiteScope remote Windows SSH files, but agentless Windows SSH is not, perform the following:

- Check that perfmon is working correctly. On the target machine, run the command **perfmon** and verify that the required perfmon objects appear. For details on how to rebuild these libraries, refer to http://support.microsoft.com/?kbid=300956.
- Check that the remote machine has a working typeperf command (sample command to test) by entering the following in the command line:

  typeperf "\Processor(_Total)\% Processor Time"

  For details, refer to http://technet.microsoft.com/en-us/library/cc753182.aspx.

Agentless SSH Fails to Retrieve Counters

In some cases, agentless SSH shows n/a for counters while perfmon gives the value as 0 for the same counters. This is the behavior for counters that are also not selectable using the perfmon utility. The reason that SSH using the SiteScope remote Windows SSH files can get values for these counters is because it bypasses perfmon and accesses them through the registry.

Windows SSH Using the SiteScope remote SSH Files is Not Working

Check that the prerequisites for Windows SSH monitoring using the SiteScope SSH files have been met. For details, see "Install SiteScope Remote Windows SSH Files" on page 661.

Error: "resize: unknown character exiting"

If SiteScope fails to create a connection using SSH and the **error.log** or **runMonitor.log** contain a server error message similar to "resize: unknown character exiting", this is probably caused by an invalid bash-related command. SiteScope supports basic bash environments only. Bash commands are usually found in the **.bashrc** file under the user default directory.

20

Working with SSH Clients

This chapter includes:

Concepts

Tasks

Concepts

Integrated Java SSH Client Overview

If you need to use Secure Shell (SSH) to connect to remote UNIX or Windows servers, SiteScope must be able to access a SSH client to make the connection and transmit data. This section contains some of the client configuration possibilities and issues involved in using SSH for SiteScope monitoring.

SiteScope provides a SSH client written in Java that is integrated into the SiteScope application. This client significantly reduces the required system resources used by SiteScope when connecting to servers by using SSH. The Java client supports both SSH version 1 (SSH1) and version 2 (SSH2) protocols as well as both password-based and key-based authentication. The SiteScope configuration for the client is identical for UNIX, Linux, and Windows SiteScope.

For details on configuring the Integrated Java SSH Client, see "How to Configure the Integrated Java SSH Client" on page 673.

This section also includes:

- "Working with the Integrated SSH Client" on page 671
- "Setting Up Key-Based Authentication" on page 672
- "Using SSH Version 2 Protocol" on page 672

Working with the Integrated SSH Client

While SSH1 and SSH2 are both Secure Shell protocols, they are considered to be two different protocols and are not compatible with each other. Some security vulnerabilities have been found in SSH1 that has resulted in SSH2 being considered the current standard. Most SSH software supports both protocols. However, to be sure that a request for a SSH connection uses SSH2 instead of SSH1, it is necessary to configure SSH clients and SSH hosts to use the same protocol version between them to communicate. In many cases, SSH1 is the default version used for connections, as it is considered the lowest common denominator between a SSH client and a SSH host.

There are two ways to force SSH2 connections:

- **Configure all SSH daemons or servers to accept only SSH2 connection requests.** This is the most secure option but may be the most time-consuming unless each server was configured for this option when it was installed and activated.
- **Configure the SSH client on the SiteScope server to only make SSH2 requests.** Requires changes only to the client on the SiteScope server. For the integrated Java SSH client, this can be controlled by a setting in the Advanced Options section on the remote server setup page.

Setting Up Key-Based Authentication

Another part of SSH security is authentication. The integrated SSH client for SiteScope can be configured to use one of two authentication options:

- **Password Authentication.** Password Authentication is the default method for SSH connections in SiteScope.
- **Key-Based Authentication.** Key-Based Authentication adds an additional level of security through the use of a passphrase and a public-private key authentication.

To use Key-Based Authentication for SSH remote servers, you must first create a pair of public/private keys. The public key resides on the remote and the private key is kept on the SiteScope machine. Both Cygwin OpenSSH and OpenSSH for Windows come with a key generation tool called ssh-keygen. The ssh-keygen tool enables you to create both protocol version 1 and version 2 keys. When setting up a UNIX or Windows remote server using the Internal Java Libraries Client, use the key generation tool called MindTerm to create a public/private key pair for RSA (version 1 and version 2) and DSA (version 2).

Using SSH Version 2 Protocol

By default, the SiteScope Java client uses the SSH1 Protocol if the server it is trying to connect to enables 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.

Tasks

How to Configure the Integrated Java SSH Client

This task describes the steps involved in configuring the integrated Java SSH client.

This task includes the following steps:

- "Select an authentication option for SSH connections" on page 673
- "Configure the SiteScope java client to use SSH2 connections only" on page 673

1 Select an authentication option for SSH connections

Select an authentication option for integrating SSH client for SiteScope: password authentication (the default method in SiteScope) or key-based authentication.

For details on how to set up key-based authentication for SSH connections, see "Set Up Key-Based Authentication" on page 674.

2 Configure the SiteScope java client to use SSH2 connections only

When configuring your remote server profile in Microsoft Windows/UNIX Remote Servers, select the **SSH version 2 only** check box in the Advanced Settings.

Set Up Key-Based Authentication

This task describes the steps involved in setting up Key-Based Authentication for SSH remote servers using MindTerm.

Note: This task is part of a higher-level task. For details, see "How to Configure the Integrated Java SSH Client" on page 673.

To create a public or private key pair:

1. Open a command window on the SiteScope server, and run the following command to launch MindTerm:

   <SiteScope root directory>\java\bin\java -jar c:\<SiteScope root directory>\WEB-INF\lib\mindterm.jar

   ---

   Note: For SiteScope 7.9.5.x and earlier, type the command: <SiteScope root directory>\java\bin\java -jar c:\<SiteScope root directory>\java\lib\ext\mindterm.jar.

   ---

2. In MindTerm, select **File** > **Create Keypair** > **DSA (or RSA)**. Also select OpenSSH .pub format.
3. The key pair is written to the **<USER_HOME>\mindterm** directory. Copy the **identity.pub** file to the **<SiteScope root directory>\groups** directory.
4. Copy the **identity.pub** file to the **<USER_HOME>/.ssh** directory on the remote machine and rename it **authorized_keys** (or **authorized_keys2** for SSH2).
5. On the remote machine, run the following command in the **<USER_HOME>/.ssh** directory, and make sure that User has read, write, and execute permissions, and that Group and Other have read permissions on the **authorized_keys** file.

6 Create a remote connection in SiteScope for the remote server using key file authentication and Internal Java Libraries.

The private key goes in the <**SiteScope root directory**>**groups** directory and the public key in the <**USER_HOME**>/**.ssh/authorized_keys** file on the remote machines.

The key generated from MindTerm is in **Openssh** format.

Note: You must verify that the server key and the MindTerm key are at the same level. For example, if the server key is 768 bit and the MindTerm key is 1024 bit, the authentication procedure fails.

To find out what your server is using:

1 Stop the sshd service on the remote server. On a Red Hat Linux server, run the command:

/etc/rc.d/init.d/sshd stop

2 Start the sshd service in debug mode on the remote server. On a Red Hat Linux server, run the command:

/usr/sbin/sshd -d

You should see output similar to Generating 768 bit RSA key.

Note: When using the **Key File for SSH connections** box in SiteScope, if there is a trailing space after the information entered, this causes an "unknown error (-1)" failure. Remove the trailing space to fix the problem.

To convert the openSSH key to SEC SSH format:

1. Create a RSA key in MindTerm (which is an openSSH key pair).
2. Run the following command on the remote server to convert the openSSH key to SEC SSH format:

   ssh-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.

21

UNIX Operating System Adapters

This chapter includes:

Concepts

Tasks

Reference

Concepts

SiteScope UNIX Operating System Adapters Overview

You can use SiteScope UNIX operating system adapters to extend SiteScope to connect to, and remotely monitor other versions of UNIX, in addition to those supported by default. This is done by configuring an adapter file to support the particular version of UNIX you want to monitor.

SiteScope uses adapter files to describe the commands that are needed to retrieve a variety of system resource information from servers running different versions of the UNIX operating system. These adapter files are written in plain text and are stored in the **<SiteScope root directory>/templates.os** directory. For a list of the default UNIX adapters that are provided with SiteScope, see "UNIX Adapters Provided with SiteScope" on page 681.

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.

Tasks

How to Add an Adapter

This task describes the steps involved in adding an adapter to specific versions of UNIX.

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 root directory**>**/templates.os** directory. The filename must use the **.config** extension.
5. Open the installation SiteScope to which you have added the new adapter file.
6. In the left pane, click **Remote Servers** to display the remote servers view.
7. In the remote servers tree, right-click **UNIX Remote Servers**, and select **New UNIX Remote Server**. The New UNIX Remote Server dialog box opens.
8. In the **Operating system** box, select the name of the UNIX adapter that you have created.
9. Click **OK**. SiteScope uses the new adapter file to try and retrieve that applicable data from the remote server.

10 If you make changes to the adapter file after you have configured one or more server connection profiles to use the adapter, you can use the **Detailed Test** option in the UNIX Remote Servers to test your adapter. After adding the remote server, the Detailed Test displays the output of the command that SiteScope is running remotely, along with SiteScope's parsing of the output.

The amount of work required to modify a particular template depends on how different the new UNIX platform is from the supported UNIX platforms.

Reference

UNIX Adapters Provided with SiteScope

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 /HP-UX.config	Adapter file for Hewlett-Packard HP/UX
HP64.config	Adapter file for Hewlett-Packard HP/UX 64-bit
ILO.config	Adapter file for Hewlett-Packard Integrated Lights-Out
Linux.config	Adapter file for Linux (Redhat and others)
MacOSX.config	Adapter file for Apple MacIntosh OS X
NonStopOS.config	Adapter file for Hewlett-Packard NonStop Operating System
OPENSERVER.config	Adapter file for SCO OpenServer
RedHatEnterpriseLinux.config	Adapter file for RedHat ES Linux
SCO.config	Adapter file for SCO UNIXWare
SGI.config	Adapter file for Silicon Graphics Irix
Sun.config / SunOS.config	Adapter file for Sun Microsystems Solaris
Tru64.config	Adapter file for Compaq Tru64 UNIX 5.x

Adapter File Format

Each UNIX platform supported for remote monitoring by SiteScope has an adapter file in the <**SiteScope root directory**>**/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.

Tip: We recommend that you use the name of the adapter file as the ID name. For example, if the name of your adapter file is linux.config, your ID would be linux.

The name is the name you want displayed in the drop-down list when adding or editing remote servers.

The rest of the template file contains groups of settings representing a single command, separated by a line of # characters. For example, the following settings represent the disk space command:

```
id=disks
command=/usr/bin/df -k
mount=6
name=1
```

where:

id=disks is the id that SiteScope uses to look up a command. This must be one of the set of SiteScope commands (see "Adapter Command List" on page 684). This entry is case sensitive.

command=/usr/bin/df -k means that the usr/bin/df -k command is run to get the information about the disks.

mount=6 and name=1 mean that the mount name is in column 6 and the name of the mount or file system is in column 1. The data names vary from command to command and are documented below.

Applying the above for the following command output:

```
Filesystem kbytes used avail capacity Mounted on /proc 0 0 0 0%
/proc /dev/dsk/c0t3d0s0 73049 42404 23341 65% /
```

where the disks command automatically skips lines not starting with (/dev) reads column 1 (/dev/dsk/c0t3d0s0) as the name of the file system, and column 6 ("/") as the mount name.

Adapter Command List

SiteScope requires settings for each the following commands to operate properly. Each command description requires an ID and a command, one or more fields to specify where the data is being read from, and optionally a set of modifiers that are used to filter the output of the command to eliminate certain sets of lines (such as header lines).

Where the variable column is used below, it means the number of the column in which the data appears, where columns are space delimited sets of data.

In addition, there are certain fields that can be optionally applied to any command description. For details, see "Optional Adapter Command Details" on page 687.

This section includes:

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 space 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.

Part VII

Preferences

22

General Preferences

This chapter includes:

Concepts

Reference

Concepts

General Preferences Overview

This section includes the following main concepts of SiteScope General Preferences:

- "Using Default Authentication Credentials" on page 692
- "Suspending Monitor Processes" on page 693
- "Web Script Monitor Files Directory" on page 693

Note: For information on general preferences relating to internationalization issues, see "Using SiteScope in an Internationalization (I18N) Environment" on page 917.

For details on configuring these preferences, see "General Preferences Page" on page 694.

Using Default Authentication Credentials

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

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

Suspending Monitor Processes

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

Web Script Monitor Files Directory

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

Note: The Web Script monitor is available only to users accessing SiteScope directly and not to users accessing SiteScope by using SAM Admin in BSM.

Reference

General Preferences Page

This page enables you to enter and view licensing information, and other general display functions, optional functions, and access options for SiteScope.

To access	Select **Preferences** context > **General Preferences**
Important information	Only an administrator in SiteScope, or a user granted **Edit general preferences** permissions, can create or make changes to General Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Configure SiteScope for a Non-English Locale" on page 920
See also	"General Preferences Overview" on page 692

Main Panel

User interface elements are described below:

UI Element	Description
VuGen scripts path root	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 784.
Default authentication user name	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	Default password 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.
Pre-emptive authorization	Displays the 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. **Default value:** Authenticate first request
SiteScope restart schedule	Enables selecting a schedule for restarting SiteScope (Off, Every 24 hours after restart, or a scheduled defined in Absolute Schedule Preferences. For details on defining a schedule, see "Absolute Schedule Page" on page 839. **Default value:** Off

UI Element	Description
Number of backups per file	Displays the number of SiteScope configuration file backups to be kept. This function helps preserve important monitor, alert, and general SiteScope configuration information. This number represents the number of backups per file that is maintained. SiteScope uses a naming convention of filename.bak.1, filename.bak.2, filename.bak.#, where 1 is the latest backup file. **Example:** You can backup files containing general SiteScope configuration information in **<SiteScope root directory>\groups**. **Default value:** 1
Locale-specific date and time	Displays dates and times in a format that is applicable to a certain locale, country, or culture. To use a different locale setting, modify the SiteScope configuration file to include the codes for the desired locale and select this option in the General Preferences Settings. For details on how to perform this task, see "How to Configure SiteScope for a Non-English Locale" on page 920. **Default value:** Selected (the default is United States format)

UI Element	Description
International version	Enables 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. or details on how to perform this task, see "How to Configure SiteScope for a Non-English Locale" on page 920. **Default value:** Not selected
Suspend all monitors	Temporarily suspends 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 affect 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 all monitors** option is enabled, the following message is displayed: SiteScope is in Suspended mode; no monitors are currently running. **Default value:** Not selected

Licenses

To use SiteScope, you must have a valid license. This pane enables you to import a license file to SiteScope, and to view the license type, status, and point consumption.

To access	Select **Preferences** context > **General Preferences** > **Licenses**
Important information	➤ If you do not have a valid license file, you can submit a request to renew or upgrade your license using the HP License Key Delivery Service site (https://webware.hp.com/Welcome.asp). ➤ The OS Instance License Usage table displays only those hosts that have at least one OS based license monitor defined on them.
See also	"SiteScope Licenses" in the *HP SiteScope Deployment Guide* PDF

User interface elements are described below:

UI Element	Description
License summary	Displays a summary of the license type and status (including the number of licensed points and points used, and the total number of OS license instances, OS instances used, and the number of license points saved by the OS instances. For a temporary or evaluation license, it also includes the number of days remaining on the license. **Note:** It does not include information from licenses that have expired, or from evaluation licenses if a general license has been imported.
License file	Enter the path to your SiteScope license file, or click the **Select** button, and select the license file. A license must be purchased if intending to use SiteScope beyond the 60-day trial period.
Import	Imports the licenses from the selected license file.

UI Element	Description
Remove License	Deletes the selected license. **Note:** When deleting a license, other licenses of the selected license type might also be removed.
Installed Licenses table	
Show expired licenses	Select to include expired licenses in the table.
Type	The type of license type imported. A license can be: ➤ **General.** Enables the standard functionality of SiteScope, based on the number of monitor points included as part of the license. A general license can be temporary (time-based) or permanent. ➤ **Evaluation.** Enables standard functionality of SiteScope and provides use of additional monitors during a free trial period (60 days with 500 monitor points). An Evaluation License cannot be renewed. ➤ **Extension.** Enables optional monitoring capabilities and solution templates. ➤ **OS Instance.** An alternative license model option calculated according to the number of OS/host instances being monitored, rather than on points for the number of monitors used. ➤ **Failover.** Enables functionality of SiteScope Failover Manager when the primary SiteScope server is down. For details on license types, see "Understanding SiteScope License Types" in the *HP SiteScope Deployment Guide* PDF.
Description	The license type and the period for which the license is valid (permanent or number of days).
Expires	The expiration date and the total number of days remaining, unless the license is a perpetual license or has expired. **Note:** When an Evaluation license is overridden by a regular points license, the license is displayed as **Expired**.

UI Element	Description
Quantity	The number of monitor points in the license you have purchased. The extension license does not increase the total number of monitor points governed by the general license key. The monitor points used for creation of optional monitor types are deducted from total monitor points included in the general license. The evaluation has a fixed value of 500 points. **Note:** ➤ For OS Instance licenses, this column displays the number of OS/host instances being monitored. ➤ For Extension licenses, this column always displays 1. Each monitor or solution template has its own point consumption which are taken from the General license points.
OS Instance License Usage Table SiteScope applies the available OS Instance licenses to the busiest hosts—the ones with the highest number of points consumed by OS Instances supported monitors only on the server. Points consumed by OS supported monitor instances are exempt, and can be used by other monitors that are not covered by the OS Instance license.	
Show top 20 hosts only	Displays the twenty busiest host servers only in the table. **Default value:** Selected
Host/OS	The name or IP address of the host machine on which OS Instances supported monitors are running.

UI Element	Description
OS Instance License Applied	Indicates whether an OS Instance license was applied on the host. For hosts on which the OS Instance license was applied, the number of points saved is displayed. The following are the OS Instance supported monitor types: ➤ CPU ➤ Directory ➤ Disk Space ➤ File ➤ HP NonStop Event Log ➤ HP NonStop Resources ➤ Memory ➤ Microsoft Archiving Server ➤ Microsoft A/V Conferencing Server ➤ Microsoft Director Server ➤ Microsoft Edge Server ➤ Microsoft Front End Server ➤ Microsoft Hyper-V ➤ Microsoft Mediation Server ➤ Microsoft Monitoring and CDR Server ➤ Microsoft Registrar Server ➤ Microsoft Windows Event Log ➤ Microsoft Windows Performance Counter ➤ Microsoft Windows Resources ➤ Microsoft Windows Services State ➤ Ping ➤ Port ➤ Service ➤ Solaris Zones ➤ UNIX Resources ➤ VMware PerformanceVMware Host CPU ➤ VMware Host Memory ➤ VMware Host Network ➤ VMware Host State ➤ VMware Host Storage ➤ VMware Performance **Note:** Points from other monitor types created on this host are not exempt.

SSH Preferences

This pane enables you to configure preferences for securely accessing a remote computer.

To access	Select **Preferences** context > **General Preferences** > **SSH Preferences**

User interface elements are described below:

UI Element	Description
SSH V2 connect timeout (seconds)	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 (seconds)	Handshake timeout (in seconds). **Default value:** 30 seconds
SSH V2 key exchange timeout (seconds)	Total number of seconds SiteScope should wait for SSH key exchange. **Default value:** 30 seconds
SSH V2 authentication phase timeout (seconds)	Total number of seconds SiteScope should wait for SSH authentication. **Default value:** 30 seconds

WMI Preferences

This pane enables you to configure preferences for using Windows Management Instrumentation (WMI) to access a remote computer. WMI is a more secure communication method than NetBIOS for gathering data from remote servers running on Windows servers.

To access	Select **Preferences** context > **General Preferences** > **WMI Preferences**
Relevant tasks	"Configure the WMI Service for Remote Monitoring" on page 596
Important information	"Monitors Supporting Windows Management Instrumentation (WMI)" on page 434

User interface elements are described below:

UI Element	Description
SiteScope NT Localhost method	Connection type method (NetBIOS or WMI) for monitoring Windows server resources on the localhost machine. **Default value:** NetBIOS
WMI query timeout (seconds)	WMI query timeout, in seconds, for each monitor run. If this box is empty, the timeout is 120 seconds. **Default value:** 120 seconds

Dashboard Monitor History View Options

This pane enables you to configure Monitor History settings to view monitor history on all monitors and monitor groups.

To access	Select **Preferences** context > **General Preferences** > **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 "Dashboard Filter Overview" on page 1289.

User interface elements are described below:

UI Element	Description
Enable monitor history view	Enables Monitor History in Dashboard. Disabling this option after it has been enabled deletes all the view data displayed in the history view. **Default value:** Not selected
Display data collected during time period	Time frame for displaying past runs. Older runs are dropped. This setting overrides any dashboard filtering. **Default value:** Past 1 hour
Monitor run status	Displays the required run status. Runs with other statuses are dropped. This setting overrides any dashboard filtering. **Default value:** Any
Maximum number of runs to display	Number of rows of data to keep in memory. **Default value:** 100000 **Minimum value:** 1000

JDBC Global Options

This pane enables you to apply global JDBC options to the SiteScope database logger, the Database Connection and Database Information tools, Database alerts, and Database monitors (Oracle Database, Database Counter, Database Query, DB2 8.x and 9.x, Technology Database Integration).

To access	Select **Preferences** context > **General Preferences** > **JDBC Global Options**

User interface elements are described below:

UI Element	Description
Connection timeout	Amount of time, in seconds/minutes/hours/days, to wait for a new SQL connection to be made. Not all SQL drivers have this function. If your SQL driver does not support this function, this parameter is ignored. **Default value:** 5 minute
Driver trace log file	Creates a driver trace log file for troubleshooting database drivers. To create the log file, enter the full path or UNC name of the driver trace file (for example, e:\mydir\myfile.log). **Note:** The target log file can contain login information, table names and queries. **Tip:** We recommend using this option for troubleshooting purposes only (it is empty by default).

LW SSO Settings

This panel enables you to change the Lightweight Single Sign-On (LW-SSO) authentication string in SiteScope.

To access	Select **Preferences** context > **General Preferences** > **LW SSO Settings**

User interface elements are described below:

UI Element	Description
LW SSO Init String	Must contain a shared string that is used by all trusted applications integrating with HP's Lightweight Single Sign On (LW-SSO). **Tip:** We recommend using at least 12 characters for the passphrase parameter. You can use any Unicode character, excluding the surrogate blocks, FFFE, and FFFF. **Note:** The default SiteScope passphrase string is not secured. To use a secured string, change the default passphrase value in SiteScope and for all HP software applications that are integrated using LW-SSO. For details on LW-SSO, see "Set Up the Authentication Strategy for Logging into SiteScope" on page 927.

23

Infrastructure Preferences

This chapter includes:

Concepts

Reference

Concepts

Infrastructure Preferences Overview

Infrastructure Preferences enable you to view and define global SiteScope settings without having to access the **master.config** file. Infrastructure Preferences are sorted and grouped into the following categories: General Settings, Server Settings, Monitor Settings, Skip Monitor Settings, Dynamic Monitoring Settings, Alert Settings, Template Settings, Persistency Settings, Report Settings, Baseline Settings, and Custom Settings.

After you edit setting values in Infrastructure Preferences, SiteScope validates that all input data is in the correct format and warns you if restarting SiteScope is required. You can restart SiteScope from the Infrastructure Preferences page.

For details on configuring infrastructure preference values, see "Infrastructure Preferences Page" on page 709.

Reference

Infrastructure Preferences Page

This page enables you to define the values of settings that determine how SiteScope runs.

To access	Select **Preferences** context > **Infrastructure Preferences**
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit infrastructure preferences** permissions can create or make changes to SiteScope Preferences and restart SiteScope from Infrastructure Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ Most Custom settings do not have a user-friendly text label and are listed only by their corresponding property name from the **master.config** file.
See also	"Infrastructure Preferences Overview" on page 708

General Settings

User interface elements are described below:

UI Element	Description
Accept untrusted SSL certificates	Enables SiteScope to accept any untrusted certificate when SSL is used. Otherwise, only certificates specified in the keystore file or that have a trust chain leading to a registered CA certificate are accepted. **Default value:** Not selected **Property name:** _sslAcceptAllUntrustedCerts
BSM downtime retrieval frequency (minutes)	Amount of time, in minutes, that SiteScope waits between querying BSM for downtime requests. **Default value:** 15 minutes

UI Element	Description
Default collection method for Microsoft Windows Resources monitor	Default collection method (pdh or registry) used for the Microsoft Windows Resources monitor when the **Use global setting** option is selected in the monitor settings. For details, see "Collection method" on page 419. **Default value:** pdh
Delay between host resolution requests (milliseconds)	Delay, in milliseconds, between successive calls to the DNS server. **Default value:** 0 milliseconds
Disable quotes for cmd.exe	Avoids wrapping parameters in quotes when running cmd.exe for specific tasks. **Default value:** Not selected **Property name:** _disableDoubleQuotesInTemplates
DNS name tags	A comma-separated list of values considered by DNS-related functionality as the DNS "name" tag. **Default value:** Name:,Nombre:,Navn:,Nome:,Nom :,Nom\u00FF: **Property name:** _dnsNameTags
DNS server tags	A comma-separated list of values considered by DNS-related functionality as the DNS "server" tag. **Default value:** Server:,Servidor:,Serveur:,Serveur\u00FF: **Property name:** _dnsServerTags
Don't check default thresholds	Checks monitor results against user selected thresholds only and not against the default SiteScope monitor thresholds. **Default value:** Selected **Property name:** _noCheckDefaultThresholds
Email character set	Character set for email generated by SiteScope in Email Preferences and Email alerts. **Default value:** If no value is entered, UTF-8 is used. **Property name:** _mailCharSet

UI Element	Description
Email subject character set	Subject character set for email generated by SiteScope in Email Preferences and Email alerts. **Default value:** If no value is entered, UTF-8 is used. **Property name:** _mailSubjectCharSet
Enable downtime mechanism	Enables the CI downtime mechanism when SiteScope is connected with BSM. SiteScope is affected by downtime if a SiteScope monitor, measurement, group, or profile CI is directly linked to a CI that BSM detects is in downtime. **Default value:** Selected **Property name:** _downtimeEnable
Enable report credentials to BSM	If selected, SiteScope sends the credentials of any host to BSM. **Default value:** Not selected **Property name:** _sendCredentials
LDAP binary attributes	SiteScope uses the names of all known binary LDAP attributes for configuration requests and responses (this affects the format of LDAP query's output). **Default value:** audio, auditingPolicy, authorityRevocationList, cACertificate, certificateRevocationList, crossCertificatePair, dSASignature, extensionData, javaSerializedData, jpegPhoto,msExchIMACL, msExchMailboxGuid, msExchMailboxSecurityDescriptor, mSMQDigests, mSMQSignCertificates, objectGUID, objectSid, personalSignature, photo, replicationSignature, thumbnailLogo, thumbnailPhoto, userCertificate, userParameters, userPassword, x500UniqueIdentifier **Property name:** _ldapBinaryAttributes
Log enabled monitors only	SiteScope does not log runs in the daily log files for monitors that have not been enabled. **Default value:** Not selected **Property name:** _onlyLogEnabledMonitors

UI Element	Description
Maximum idle threads per pool	Maximum number of idle threads per thread pool. **Default value:** 100 **Note:** You must restart SiteScope if you change this setting. **Property name:** _threadPoolMaxIdle
Maximum idle time (ms) for a thread in the pool	Amount of time, in milliseconds, to wait before SiteScope cleans idle thread pools. **Default value:** 600000 milliseconds (10 minutes) **Property name:** _threadPoolMaxIdleTime
Maximum idle time for perfex process in minutes	Amount of time, in milliseconds, to wait before SiteScope cleans idle perfex processes. Cleaning processes improves the memory footprint on the SiteScope machine. **Default value:** 60 minutes **Property name:** _perfexProcessMaxIdleTime
Maximum processes per pool	Maximum number of processes per process pool. **Default value:** 200 **Note:** You must restart SiteScope if you change this setting. **Property name:** _processPoolMaxPerPool
Maximum size of data integration sample's queue	Upper limit of the data integration sample's queue. When this limit is reached, old samples are discarded. **Default value:** 1000 **Property name:** _dataSamplesQueueMaxSize
Monitor delay between refresh (milliseconds)	Amount of time, in milliseconds, to wait before running a monitor after it has already been run since startup. **Default value:** 1000 milliseconds **Property name:** _monitorDelayBetweenRefresh

UI Element	Description
NT SSH timeout (seconds)	Amount of time, in seconds, to wait for an SSH connection to remote Windows servers before timing out. **Default value:** 60 seconds **Property name:** _NTSSHTimeout
Number of open port tries	Maximum number of attempts to open a reserved port in the 811-1024 range for rlogin and rsh remote access methods. **Default value:** 25 **Note:** You must restart SiteScope if you change this setting. **Property name:** _localPortRetryCount
Number of samples to discard if queue max size reached	The number of samples to discard if the queue size maximum has been reached. **Default value:** 500 **Property name:** _dataSamplesQueueDiscardSamples
Numeric values format	Format of numeric values when converting to string representation. **Default value:** #.## **Property name:** _noScientificNotation **Tip:** For more detailed information on numeric values format, refer to the HP Software Self-solve knowledge base (http://h20230.www2.hp.com/selfsolve/document/KM305059). To enter the knowledge base, you must log on with your HP Passport ID.
Perfex timeout (seconds)	Amount of time, in seconds, to wait for perfex to attempt to make a connection or to attempt to run a monitor before timing out. **Default value:** 120 seconds **Property name:** _perfexTimeout

UI Element	Description
Power Shell execute command	To enable use of the Microsoft Exchange 2007/2010 monitor on 64-bit version of Windows 2003, Windows 2008, or Windows XP (since a 32-bit application cannot access the system32 folder on a computer that is running a 64-bit version of Windows Server 2003, 2008, or of Windows XP), perform the following: ➤ Apply the Microsoft hotfix available from http://support.microsoft.com/?scid=kb;en-us;942589 ➤ Enter the PowerShell execute command. For example: C:\Windows\Sysnative\WindowsPowerShell\v1.0\powershell.exe **Note:** Symlink Sysnative is not available by default on Windows 2003 or Windows XP.
Processes wait for server timeout in multithreading	If selected, a separate thread is opened for each process that is waiting for a server timeout to close the connection, or for an answer to return the process to the pool. This setting increases the thread count and used memory if many servers are down. When this setting is cleared (recommended), SiteScope uses only one thread to manage such processes. **Default value:** Not selected
Process pool kill timeout (milliseconds)	Amount of time, in milliseconds, to wait before SiteScope kills a non-responsive process. This is to avoid killing processes on every timeout. **Default value:** 60000 milliseconds (the maximum recommended value is 180000 milliseconds) **Note:** You must restart SiteScope if you change this setting. **Property name:** _processPoolKillTimeout

UI Element	Description
Recursive 'depends on'	Enables recursion in the monitor **Depends on** box. This means that subgroups become disabled when the parent group is disabled because of a dependency. By default, only the immediate group impacted by the dependency is disabled. **Default value:** Not selected **Note:** You must restart SiteScope if you change this setting. **Property name:** _dependsOnRecursive
Send remote server display name to BSM	Sends the remote server display name to BSM instead of the remote server host name. It is preferable to use this setting when DNS resolution is disabled. **Default value:** Not selected **Property name:** _sendRemoteServerDisplayNameToBAC
SiteScope sleep delay (milliseconds)	Amount of time, in milliseconds, of the sleep interval in the main thread. **Default value:** 180 milliseconds **Note:** You must restart SiteScope if you change this setting. **Property name:** _monitorProcessCheckDelay
SiteScope tree refresh rate (seconds)	Amount of time, in seconds, to wait between refreshing the SiteScope tree. The minimum value is 30 seconds. **Default value:** 60 seconds **Property name:** _sisTreeRefreshRateSecs
Sleep interval on error (milliseconds)	Amount of time, in milliseconds, to wait before rerunning a monitor using the **Verify error** option. **Default value:** 5000 milliseconds **Property name:** _verifySleepDuration

UI Element	Description
SSH prompt timeout (milliseconds)	Amount of time, in milliseconds, for SiteScope to wait for an SSH connection prompt to finish before running the first command. **Default value:** 3000 milliseconds **Property name:** _waitSshPromptTimeout
Time period for cleaning idle SSH connections from pool (minutes)	Amount of time, in minutes, for cleaning idle SSH connections from the SSH connections pool. **Default value:** 10 minutes **Property name:** _SSHConnectionIdleCleanTimeMinutes
Time zone offset	Manually sets the time zone offset, in hours, from Greenwich Mean Time (GMT). You can enter both positive and negative, integer and non-integer values. **Default value:** -999 (no offset) **Example:** In Eastern US (EST), where the time zone offset is GMT -5, you should enter the value 5. In central Europe, where the time zone offset is GMT +2, enter the value -2. **Note:** You must restart SiteScope if you change this setting. **Property name:** _timeZoneOffset
Traceroute command	(For Unix) Path to the traceroute command to override the default for the platform. **Default value:** No value **Property name:** _tracerouteCommand
Wait for SSH connection prompt	SiteScope waits for the end of the SSH connection prompt before it starts to run the first command. Select this setting if the SSH remote server has a long start prompt. **Default value:** Not selected **Property name:** _readUntilPromptFound

Server Settings

User interface elements are described below:

UI Element	Description
Host name override	Overrides the SiteScope host name for BSM. **Default value:** No value **Property name:** _sisHostNameOverride
Kill processes	Kills child processes when the SiteScope process is stopped. **Default value:** Selected **Property name:** _killProcesses
Maximum monitor processes	Maximum number of monitor processes in the process pool. **Default value:** 100 **Note:** You must restart SiteScope if you change this setting. **Property name:** _maxMonitorProcesses
Maximum monitor running	Maximum number of running monitor processes in the queue. **Default value:** 400 **Note:** You must restart SiteScope if you change this setting. **Property name:** _maxMonitorsRunning
Minimal monitor run interval (seconds)	Minimal possible monitor frequency. If you try to create a monitor with frequency less then this frequency, a validation error is displayed. **Note:** You must restart SiteScope if you change this setting. **Default value:** 15 **Property name:** _monitorMinInterval

UI Element	Description
Prefer IP version 6 addresses	If a host is resolved to both IPv6 and IPv4, IPv6 is used. For details on support for IPv6 in SiteScope, see "IP Version 6 Support in SiteScope" on page 629. **Note:** You must restart SiteScope if you change this setting. **Default value:** Not selected **Property name:** _preferIPV6Address
SiteScope heartbeat restart timeout (minutes)	Maximum time, in minutes, before SiteScope restarts itself when no heartbeat events are detected. **Note:** You must restart SiteScope if you change this setting. **Default value:** 5 minutes **Property name:** _heartbeatRestartTimeout
SiteScope restart timeout (minutes)	Maximum time for SiteScope to restart itself. **Default value:** 15 minutes **Property name:** _restartTimeout
SiteScope shutdown timeout (seconds)	Amount of time, in seconds, that SiteScope should wait to shutdown before timing out. **Default value:** 60 seconds **Property name:** _shutdownTimeout
Startup script	Runs this script whenever SiteScope starts up, regardless of the platform or procedure used to start SiteScope. (Empty=none) **Default value:** No value **Property name:** _startupScript

Monitor Settings

User interface elements are described below:

UI Element	Description
Additional error tokens	Additional list of keywords that should be handled as signs of failure during server output parsing. **Default value:** Failed to .* Error code: **Property name:** _scriptMonitorErrorMsgs2
Additional event log name	Enables the Microsoft Windows Event Log monitor to monitor event logs other than the standard logs, by entering additional log names. **Default value:** No value **Property name:** _additionalEventLogNames
Additional event types	Enables the Microsoft Windows Event Log monitor to monitor event types other than the standard application, system, or security logs, by entering additional event type categories. **Default value:** No value **Property name:** _additionalEventTypes
Allow all request headers in URL specific monitors	Allows all request headers in URL specific monitors. **Default value:** Not selected **Property name:** _urlOtherHeader=
Browsable EXE timeout (milliseconds)	Maximum amount of time, in milliseconds, to wait for retrieving counter information and for running the monitor. This setting only applies to executable-based browsable monitors, such as SAP, Sybase, and DB2 8.x and 9.x monitors. **Default value:** 45000 **Property name:** _browsableExeTimeout

UI Element	Description
Browsable monitors - If in error, send status of all counters to BSM	When a browsable monitor is in error status, SiteScope only sends the list of counters in error and their current values to BSM. At other times (when the monitor is in good status), SiteScope forwards all the counter names and values to BSM. If selected, SiteScope sends all the counters (the ones in error, and the ones with good status) and their values to BSM even during error. **Default value:** Not selected **Property name:** _isSendStatusOfAllBrowsableCountersToBAC
CPU error at 100%	CPU monitor switches to the default error status when CPU utilization reaches 100% on the target machine. **Default value:** Selected **Property name:** _cpuEnableErrorAt100
CPU maximum units	Maximum number of CPU units supported by the CPU monitor. **Default value:** 16 **Property name:** _cpuMaxProcessors
DB maximum columns	Maximum number of columns processed by DB monitors. **Default value:** 10 **Property name:** _databaseMaxColumns
DB maximum rows	Maximum number of rows processed by DB monitors. **Default value:** 1 **Property name:** _databaseMaxRows
DB maximum value length	Maximum length, in characters, of the data processed by DB monitors. **Default value:** 200 **Property name:** _databaseMaxSummary

UI Element	Description
Default precision	The default precision for floating-point values processed by some monitors. **Default value:** 0 (disabled) **Property name:** _defaultPrecision
Dialup options	Options for **dialup.exe** when running it from the Microsoft Windows Dial-up monitor. Set to -silent to have the modem dial silently. Set to -debug to enable dialup debugging. **Default value:** 0 **Property name:** _dialupOptions
Empty last line reading	Includes the last empty line in the Script monitor output. **Default value:** Not selected **Property name:** _enable_script_monitor_non_empty_last_line_reading
Enable/disable description mandatory	Enables you to make adding a description a required field when enabling or disabling an alert or monitor. **Default value:** Not selected **Property name:** _enableDisableDescriptionMandatory
Enable JDBC logging	Enables JDBC search results logging for the Link Check monitor. **Default value:** Not selected **Property name:** _linkMonitorJdbcEnabled
Error tokens for Script monitor	List of keywords that should be handled as signs of failure during server output parsing. **Default value:** not found, Not Found, denied, Denied, cannot execute such file or directory **Property name:** _scriptMonitorErrorMsgs
Event log messages to save	Number of Microsoft Windows Event Log descriptions to save when saving diagnostic text for alerts. **Default value:** 10 **Property name:** _eventLogMessagesToSave

UI Element	Description
Exclusive monitor timeout (seconds)	Maximum amount of time, in seconds, that exclusive monitors must wait for other monitors to finish before running. The only monitor affected by this is the Microsoft Windows Dial-up monitor. **Default value:** 120 seconds **Property name:** _exclusiveMonitorTimeout
FTP content match maximum size	Maximum size of the buffer used to match FTP content. **Default value:** 50000 **Property name:** _ftpContentMatchMax
FTP download limit	Maximum number of bytes downloaded from each file to match. **Default value:** -1 (no limit) **Property name:** _ftpDownloadLimit
FTP maximum threads	Maximum number of simultaneous FTP worker threads. **Default value:** 1 **Property name:** _ftpMaxThreads
HTTP content match display limit	Maximum number of bytes to display for URL monitor content match. **Default value:** 150 **Property name:** _urlContentMatchDisplayMax
HTTP content match limit	Maximum number of bytes to check for URL monitor content match. **Default value:** 50000 **Property name:** _urlContentMatchMax

UI Element	Description
Initial monitor delay (seconds)	The time, in seconds, over which to randomly schedule monitor updates after a SiteScope restart. When changing a monitor's frequency so that its next run occurs immediately (for example, if a monitor has not run in 5 minutes, and you change the frequency to less than 5 minutes), SiteScope randomly schedules the next run during the specified period. **Default value:** 600 seconds **Property name:** _initialMonitorDelay
Mail attachment content support base64	Supports mail attachment content-transfer-encoding with base64 for the Mail monitor. **Default value:** Not selected **Note:** You must restart SiteScope if you change this setting. **Property name:** _mailAttachmentBase64Support
Maximum browsable counters to be selected	Maximum number of browsable counters that can be selected from the browsable tree. If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved. **Note:** When a browsable monitor is deployed in a template, the number of counters that match the selected patterns are limited by the **_maxCountersForRegexMatch** parameter in the **master.config** file. If, during deployment, the number of counters that match the patterns exceed this value, only the number of counters up to this value is saved. Therefore, we recommend using the same value for this setting and the **_maxCountersForRegexMatch** parameter. The default value for both of these parameters is 1000. **Default value:** 1000 **Property name:** _browsableContentMaxCounters

UI Element	Description
Maximum counters for application monitors	Maximum number of counters that can be selected for application monitors. **Default value:** 100 **Property name:** _ApplicationMonitorMaxCounters=100
Maximum counters for SNMP by MIB monitor	Maximum number of counters supported by the SNMP by MIB monitor. **Default value:** 32 **Property name:** _maxSNMPbyMIBCounters
Maximum Windows Performance Counter monitor counters	Maximum number of counters for each instance of a Microsoft Windows Performance Counter monitor. **Default value:** 8 **Property name:** _NTCounterMonitorMaxCounters
Microsoft Windows Media Server monitor service names	Service names to monitor using the Microsoft Windows Media Server monitor. **Default value:** Windows Media Services (this includes Windows Media Station Service and Windows Media Unicast) Service) **Property name:** _counterObjectsWindowsMediaMonitor
MQ Server CCSID	Default WebSphere MQ server CCSID in SiteScope. **Default value:** No value **Property name:** _mqServerCCSID=
MS Media Player 9 account blocked	Select this option and add the account directory path to the **MS Media Player 9 account directory** box if your Media Player account stops working with a 17999 error. **Default value:** Not selected **Property name:** _MediaPlayer9AccountBlocked

UI Element	Description
MS Media Player 9 account directory	Enter the Media Player account directory if you get a 17999 error for the Media Player monitor. **Default value:** No value **Example:** C:\Documents and Settings\<USER>\Local Settings\Application Data\Microsoft\Windows Media\9.0 **Property name:** _MediaPlayer9AccountBlockedDir
Network Bandwidth monitor sanity check	Performs a sanity check on the Network Bandwidth monitor. **Default value:** Selected **Property name:** _performNetworkBandwidthSanityCheck
Real Media Server monitor service names	Service names to monitor using the Real Media Server monitor. **Default value:** RMServer **Property name:** _counterObjectsRealMonitor
Run script through perfex tool	Runs the script through the perfex tool. **Default value:** Selected **Property name:** _scriptRunThroughPerfex
Script monitor output limit	Number of lines to save from Script output after launching the Script monitor. **Default value:** 25 **Property name:** _scriptMonitorLinesToSave
Script monitor replacement strings	Stores a list of space-separated strings which are parameter tags in the remote script. When the Script monitor is run, it replaces parameters tags from the script command with actual parameter values from monitor preferences. **Default value:** $ % **Property name:** _scriptMonitorReplacementChars **Example:** If the script command is test $ %, replacement chars are $ %, and parameters are Param1 Param2, the monitor runs the following command: test Param1 Param2.

UI Element	Description
Simultaneously running DNS monitors	Maximum number of DNS monitors that can run simultaneously. This is relevant only when using the **roundTripTime** counter. The NSLookup operation can load the operating system and affect the values. **Default value:** 0 (0 means that the number of simultaneous DNS monitors is unlimited) **Note:** You must restart SiteScope if you change this setting. **Property name:** _maxDnsMonitorsRunning
SNMP monitors maximum number	Maximum number of SNMP monitors that can run at any given time. **Default value:** 10 **Note:** You must restart SiteScope if you change this setting. **Property name:** _snmpMonitorMaximum
SNMP session closure timeout (milliseconds)	Maximum amount of time, in milliseconds, that SiteScope waits before closing the SNMP session. **Default value:** 30000 **Property name:** _maxSNMPCloseSessionTimeMillis
SNMP Trap encoding	SNMP Trap encoding for the SNMP Trap monitor. Empty=ISO8859-1. **Default value:** ISO8859-1 **Property name:** _snmpTrapEncoding
SNMP Trap monitor log limit	Maximum number of lines to look through SNMP Trap log for the SNMP Trap monitor. This box is filled only if **Run Alerts** is set to **Once, after all SNMP Traps have been checked** in the SNMP Trap monitor page. **Note:** Setting a high limit may increase the size of the **SiteScope.log** or **RunMonitor.log**. **Default value:** 1000 **Property name:** _SNMPTrapMonitorDetailsMax

UI Element	Description
Use DNS Java library	Activates Java DNS functionality instead of using the default perfex setting. In some cases, DNS response times are faster than the perfex response. **Default value:** Not selected **Property name:** _useDNSJava
Use sequence of requests for SNMP by MIB	Activates a new mode of requests for the SNMP by MIB monitor. Using this option, SiteScope executes a separate request to the remote server for each OID counter from the monitor. **Default value:** Not selected **Property name:** _sequenceSNMP
Web Script monitor queue size	The size of the Web Script monitor queue. **Default value:** 20 (maximum value: 40) **Property name:** _maxWebScriptMonitorsRunning
Web Script monitor queue timeout (seconds)	The amount of time, in seconds, for the Web Script monitor to wait in the queue before timing out. **Default value:** 120 seconds **Property name:** _webScriptMonitorsWaitingInQueueTimeout
Web Service monitor maximum read length (bytes)	Maximum amount of data, in bytes, to read from the log file for the Web Server monitor. **Default value:** 50000 bytes **Property name:** _maxAmountToRead

UI Element	Description
Web Service monitor timeout (seconds)	Maximum amount of time in seconds for the Web Server monitor to run. **Default value:** 30 seconds **Property name:** webServiceTimeout=30
Web Service Monitor use common content match	Content match behavior was changed for the Web Service monitor in SiteScope 10.12. This setting enables Web Service monitors defined prior to SiteScope 10.12 to match the correct value. This means that Web Service monitors behave in the same way as other monitors where content matching is used. Clear the setting to revert to the old content match behavior. **Default value:** Selected

Skip Monitor Settings

User interface elements are described below:

UI Element	Description
Disable period of skip monitor (seconds)	The period of time, in seconds, that a monitor is disabled after the maximum number of monitor skips (defined in **Maximum monitor skips**) has been exceeded. **Default value:** 360 seconds **Property name:** _monitorDisablePeriodOnSkip
Maximum monitor skips	Maximum number of consecutive monitor skips before a monitor is disabled. **Default value:** 10 **Note:** You must restart SiteScope if you change this setting. **Property name:** _maxMonitorSkips
Send email to administrator if monitor is disabled after a skip	SiteScope sends an email to the administrator if a monitor is disabled after the maximum number of consecutive monitor skips has been exceeded. **Default value:** Not selected **Property name:** _emailSkipNotification
Shutdown on monitor skips	SiteScope shuts down with an error if a monitor exceeds its maximum skip count. **Default value:** Not selected **Property name:** _shutdownOnSkips

Dynamic Monitoring Settings

User interface elements are described below:

UI Element	Description
Dynamic monitoring core thread pool size	Number of threads in pool that will be created for new dynamic monitors changes check tasks. **Default value:** 5 **Note:** You must restart SiteScope if you change this setting. **Property name:** _dynamicMonitoringCoreThreadPoolSize
Dynamic monitoring maximum queue size	Maximum number of new dynamic monitors changes check tasks that can be added to the queue. If all the core threads are busy, the new tasks are added to the queue until the maximum queue size is reached. **Default value:** 5000 **Note:** You must restart SiteScope if you change this setting. **Property name:** _dynamicMonitoringMaxQueueSize
Dynamic monitoring maximum thread pool size	Maximum number of threads in pool that will be created for new dynamic monitors changes check tasks. These extra threads are created only if all the core threads are busy and the maximum queue size has been reached. **Default value:** 30 **Note:** You must restart SiteScope if you change this setting. **Property name:** _dynamicMonitoringMaxThreadPoolSize

Alert Settings

User interface elements are described below:

UI Element	Description
Alert attempt delay (seconds)	Amount of time, in seconds, to wait between each attempt to send a Post Alert. **Default value:** 120 seconds **Property name:** _postAttemptDelay
Maximum alert threads	Maximum number of alert threads in the pool. **Default value:** 100 **Property name:** _threadPoolAlertMaxThreads
Maximum runs for Post action	Maximum number of attempts to send a Post Alert. **Default value:** 4 **Property name:** _postAttempts
Maximum script alert processes	Maximum number of Script Alert processes that can run simultaneously. **Default value:** 25 **Property name:** _maxScriptAlertProcesses
Maximum sound alert length (milliseconds)	Maximum length of time, in milliseconds, of the Sound Alert sound. **Default value:** 0 **Property name:** _AudioSleepTime
Pager delay (seconds)	Delay between pager signals when using a Pager Alert. **Default value:** 5 **Property name:** _delayBetweenPages

Template Settings

User interface elements are described below:

UI Element	Description
Allow creation of template monitors directly under template entity	Enables adding a monitor directly under a template without creating a group in the template. **Note:** You must restart SiteScope if you change this setting. **Default value:** Not selected **Property name:** _allowTemplateMonitorDirectlyUnderTemplate

Persistency Settings

User interface elements are described below:

UI Element	Description
Maximum changes per persistency delta file	Maximum number of persistency changes kept in each persistency delta file. **Default value:** 51 **Note:** You must restart SiteScope if you change this setting. **Property name:** _PersistencyMaxChangesInDeltaFile
Maximum persistence history items	Maximum number of history items kept in persistence. **Default value:** 1000 **Property name:** _PersistencyMaxHistoryItems
Maximum persistence history size	Maximum size, in bytes, of persistence history. **Default value:** 20000 **Note:** You must restart SiteScope if you change this setting. **Property name:** _PersistencyMaxHistorySize

UI Element	Description
Maximum persistency delta files	Maximum number of delta files kept in persistence. After this number is reached, a new snaphot (.ssf) file is created with all the persistency objects. All old .ssf files are moved to the history folder. **Default value:** 100 **Property name:** _PersistencyMaxDeltaFiles
Maximum temp directory size	Maximum size, in kilobytes, of the temp directory. **Default value:** 10000 **Note:** You must restart SiteScope if you change this setting. **Property name:** _tempDirMaxSize

Report Settings

User interface elements are described below:

UI Element	Description
Default time length for report (hours)	Default time period for including monitoring data in a Quick or Alert report. **Default value:** 1 hour **Property name:** _quickReportDefaultTimePeriod
Include alert.log.old in report	Includes the **alert.log.old** file in the Alert Report. **Default value:** Selected **Property name:** _includeAlertLogOld
Maximum errors in monitor history report	Maximum number of errors shown in the monitor history report. **Default value:** 100 **Property name:** _maxReportErrors
Maximum samples in the history report	Maximum number of samples (readings or lines) in the history report. **Default value:** 100 **Property name:** _reportMaxBuckets
Maximum warnings in monitor history report	Maximum number of warnings shown in the monitor history report. **Default value:** 100 **Property name:** _maxReportWarnings
Use advanced sampling algorithm in report	Defines the time between samples in the report as the minimum of all reported monitor frequencies. **Default value:** Not selected **Property name:** _useReportAdvancedSamplingAlgorithm

Baseline Settings

User interface elements are described below:

UI Element	Description
Activation thread priority	Priority assigned to the activation thread. The priority, if specified, must be between 1-10, inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baselines are activated. Keep the priority as low as possible, so as not to interfere with SiteScope online functionality. **Default value:** 1 (low priority) **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningActivationThreadPriority
Automatically create an error boundary if no error thresholds are defined	Automatically creates a baseline threshold using the error boundary offset value when no error thresholds have been defined for a monitor. **Default value:** Selected **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningAutomateUpperBoundCreation
Calculation thread priority	Priority assigned to the calculation thread. The priority, if specified, must be between 1-10 inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baseline calculations take to complete. Keep the priority as low as possible, so as not to interfere with SiteScope online functionality. **Default value:** 1 (low priority) **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningCalculationThreadPriority

UI Element	Description
Failed parsings handler thread priority	Priority assigned to the failed parsing thread handler. The priority, if specified, must be between 1-10 inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baseline calculations take to complete. Keep the priority as low as possible, so as not to interfere with SiteScope online functionality. **Default value:** 1 (low priority) **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningFailedParsingHandlerThreadPriority
Include today's data in calculation	Specifies whether to include the current day's data in the baseline calculation. **Default value:** Selected **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningCalculationIncludesToday
Interval for saving baseline data to disk (minutes)	Interval, in minutes, used by SiteScope to save baseline data accumulated in the memory to the disk. A shorter interval reduces the memory consumption, but increases the vulnerability to failures and reduces performance. **Default value:** 30 minutes **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningSaveAccumulatedDataIntervalMinutes

UI Element	Description
Maximum number of days to include in calculation	Number of days of historical data that are included in baseline calculations. The higher the number, the more precise the baseline result, but the calculation takes more time and uses more disk space. Data that is older than this value is not included in the calculation. For more details on the calculation model, see "How SiteScope Calculates Thresholds" on page 412. **Default value:** 30 days **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningDaysToIncludeInCalculation
Maximum number of percentile ranges	Limits the number of percentile ranges displayed in the Percentile Ranges Mapping Table. **Default value:** 8 **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningMaxNumberOfPercentilesRanges
Minimum number of days required for baselining	Minimum number of days that the monitors must have run for SiteScope to calculate the baseline. **Default value:** 14 days **Minimum value:** 1 (if you enter a value of less than 1, the default value is used instead). **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningMinimumNumberOfDays

UI Element	Description
Minimum number of samples required for baselining	Minimum number of samples required for SiteScope to calculate the baseline. **Default value:** 2016 (the number of samples produced for a monitor running over a two week period, where the monitor runs every 10 minutes) **Minimum value:** 1 (if you enter a value of less than 1, the default value is used instead). **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningMinimumNumberOfSamples
Offset for calculating error boundary	Offset value to use for calculating the error boundary. The baseline threshold is multiplied by this value when: ➤ The **Automatically create Error Threshold Boundary if no error thresholds are defined** option is selected (see below), or ➤ The current most extreme error threshold is less extreme than the calculated baseline threshold. **Default value:** 0.3 **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningUpperBoundOffset
Parsing chunk size	Number of monitors that are handled simultaneously by the log file parser. The higher the number, the faster the baselining calculation, but more file handlers are used. **Default value:** 100 **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningParsingChunkSize

UI Element	Description
Parsing thread priority	Priority assigned to the parsing thread. The priority, if specified, must be between 1-10 inclusive. If not specified, the priority is set to 1. Generally, the higher the priority, the faster the baseline calculations take to complete. Keep the priority as low as possible, so as not to interfere with SiteScope online functionality. **Default value:** 1 (low priority) **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningParsingThreadPriority
Percentile of discarded samples	Percentile of the most extreme samples (considered "noise" measurement samples) that are not included in the baseline calculation. **Default value:** 2.0 **Note:** You must restart SiteScope if you change this setting. **Property name:** _baseliningNoiseMarginPercentile

Custom Settings

Note: Most Custom settings do not have a user-friendly text label and are listed only by their corresponding property name from the **master.config** file. These settings are not included in the documentation.

User interface elements are described below:

UI Element	Description
Auto Deployment Check Frequency (seconds)	Time interval in seconds that the auto template deployment xml files in the **persistency\autodeployement** directory are deployed. For details on the feature, see "Auto Template Deployment" on page 1053. **Default value:** 120 **Property name:** _autoDeploymentCheckFrequency
Topology resolving frequency (minutes)	Amount of time, in minutes, to wait between checking the topology of the server being monitored. If this time is exceeded during a monitor run, the monitor creates the topology again in BSM's RTSM. **Default value:** 120 minutes **Property name:** _topologyResolvingFrequencyInMinutes

24

Integration Preferences

This chapter includes:

Concepts

Tasks

Reference

Concepts

Integration Preferences Overview

Using the Integration Preferences interface, you can create integration instances, enabling SiteScope to report monitoring data to the following applications:

- **HP Business Service Management**
  - For details on understanding the integration, see "Working with Business Service Management (BSM)" on page 269.
  - For details on the integration preferences, see "HP Business Service Management Integration Preferences" on page 743.
  - For user interface details, see "BSM Integration Preferences Dialog Box" on page 760.
- **HP Diagnostics**
  - For details on understanding the integration, see "Diagnostics Integration Overview" on page 746.
  - For user interface details, see "Diagnostics Integration Preferences Dialog Box" on page 771.
- **HP Operations Manager**
  - For details on understanding the integration, see "Understanding How SiteScope Communicates with HPOM and BSM" on page 308.
  - For details on the HP Operations Manager integration preferences, see "HP Operations Manager Integration Overview" on page 748.
  - For user interface details, see "HP Operations Manager Integration Dialog Box" on page 776.

- **Generic data applications**
  - For details on understanding the integration, see "Generic Data Integration Overview" on page 749.
  - For user interface details, see "Data Integration Preferences Dialog Box" on page 766.

HP Business Service Management Integration Preferences

To enable logging of SiteScope monitor data to BSM, the SiteScope must be configured as a data collector for BSM. This involves adding a SiteScope to the System Availability Management Administration (SAM Admin) page in the BSM. After the SiteScope is added and a connection is established, a BSM Integration Preference appears in the Integration Preferences page that includes the relevant configurations as entered in the New SiteScope Page in SAM Admin.

You use the Integration preference to:

- Modify the available integration settings.
- Disable logging all data to BSM. This includes topology reporting.
- Create an integration for an empty SiteScope profile. If when adding the SiteScope to SAM Admin, the SiteScope was not accessible to BSM (for example, when working in HP Software-as-a-Service), you add a SiteScope with an **Inaccessible profile** to SAM Admin. You then configure the connection and the integration in the Integration Preferences. For details on this task, see "How to Configure SiteScope-BSM Integration Preferences for Inaccessible Profiles" on page 751.

If the BSM Server to which you are connecting is on a different machine than the BSM Server that SiteScope reports data, you must provide connection information for both servers under the **Main Settings** in SiteScope's Integration Preferences, or in the **Distributed Settings** in SAM Admin's New SiteScope Page.

For details on configuring these preferences, see "BSM Integration Preferences Dialog Box" on page 760.

This section contains the following topics:

Using SSL for SiteScope-BSM Communication

You can use Secure Sockets Layer (SSL) to transmit data from SiteScope to the BSM server. If you have installed a certificate signed by a root Certificate Authority on the BSM server, no additional setup is required on the SiteScope server. If you are using a self-signed certificate on the BSM server and want to use that certificate for secure communication with SiteScope, you must perform the appropriate step below:

- For BSM server that requires SSL, see "How to Connect SiteScope to a BSM Server That Requires SSL" on page 296.
- For BSM server that requires a client certificate, see "How to Connect SiteScope to a BSM Server That Requires Client Certificate" on page 297.

Note:

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

Changing the Gateway Server to Which SiteScope Sends Data

You can change the Gateway Server to which a SiteScope reports its data. Generally, this is applicable only if you are working with a BSM 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 Service Management machine name/IP address** box in the Integration Preferences page. You must also update the SiteScope settings with the **Gateway Server** name in SAM Admin.

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

Compressing SiteScope Data Sent to BSM

By default, when data is sent from the SiteScope server to BSM it is sent uncompressed. To enable data compression of SiteScope monitor (ss_monitor_t) and SiteScope metric (ss_t) samples, set the property **_compressDataInGzipFormat=** to **true** in the **<SiteScope root directory>\groups\master.config** file. When this setting is enabled, SiteScope data is compressed in gzip before it is sent to BSM (where it is decompressed). Note that data compression can be used only when SiteScope is reporting to BAC 8.05 or later, or BSM 9.01 or later.

Troubleshooting and Limitations

For information about troubleshooting reporting data to BSM, see "Troubleshooting and Limitations" on page 304.

Diagnostics Integration Overview

SiteScope forwards data to HP Diagnostics enabling you to see a more complete view of the application servers that are monitored by Diagnostics. The data can provide insight into the infrastructure components onto which the application servers are deployed.

For example, integrating data from the SNMP by MIB monitor can help determine problems with the infrastructure on which the application server runs.SiteScope forwards data on groups, monitors, and measurements. HP Diagnostics can read the data sent from SiteScope and present the data in its reports and graphs.

For user interface details, see "Diagnostics Integration Preferences Dialog Box" on page 771.

Units of Measurements in Diagnostics

SiteScope generates a file **<SiteScope root directory>/conf/integration/data_integration_uom.xml** that controls the mappings of SiteScope monitors to Diagnostics metrics and the units of measurement used for the metrics. Diagnostics accepts data from SiteScope only if the data is associated with a unit of measurement that Diagnostics can recognize. SiteScope units are captured from the monitored source and may need to be mapped to the appropriate Diagnostics unit of measurement. The units of measurements used by SiteScope monitors vary, depending on the type of data being monitored. For example, the unit of measurement used for the CPU monitor is a percentage and the unit of measurement used for the Disk Space monitor is number of bytes. It is therefore recommended that you modify the xml file as needed so that Diagnostics recognizes the unit of measurement to use for the monitor data coming from SiteScope.

When new monitors are added to the SiteScope that report data to Diagnostics, it is recommended that you edit the Diagnostics Integration Preference and click the **Generate UOM XML** button. SiteScope generates a list of currently deployed monitors and their corresponding metrics. This list merges with the **<SiteScope root directory>/conf/integration/data_integration_uom.xml** file and updates only those values in the xml file that were not manually changed. If any values were manually changed in the xml file, those values are not updated and are preserved. This merge of information on units of measurements occurs when you click this button and on each SiteScope restart.

For a reference detailing the XML tags, elements, and attributes included in the integration file that SiteScope forwards to HP Diagnostics, see "XML Tag Reference for Generic Data and Diagnostics Integrations" on page 753.

HP Operations Manager Integration Overview

To provide visibility of SiteScope servers and monitors to HP Operations Manager (HPOM) and Operations Management in BSM, the HP Operations agent must be installed and configured on the SiteScope server. The HP Operations agent sends event data to the HPOM management server and to Operations Management. It also acts as a data storage for metrics data collected by SiteScope. The agent must be connected to the HPOM/BSM Server, and event or metrics integration with HP Operations Manager must be enabled.

Note: This integration replaces the need to install the HP SiteScope Adaptor on the HPOM server that was required for the earlier integration solution when using the basic alert script mechanism.

- **Event Integration.** SiteScope events are triggered when there is a change in SiteScope monitor metric status (**good**/**warning**/**error**) or when a SiteScope alert is triggered. SiteScope sends events by writing them to a log file which is monitored by the HP Operations agent. The agent reads the data and converts it to events, which it forwards to the HPOM/BSM server. For details on sending events, see "Sending Events" on page 313.
- **Metrics Integration.** SiteScope metrics data is collected from the HP Operations agent data storage by HPOM for use in Performance Manager graphs, and by BSM for use in Performance Perspective in Operations Management. For details on reporting metrics, see "Reporting Metrics Using the HP Operations Agent" on page 322.

For details on configuring the HP Operations Manager integration settings, see "HP Operations Manager Integration Dialog Box" on page 776.

Generic Data Integration Overview

This is a generic integration that can be used to forward data to another application. That application must be able to receive the XML files that SiteScope forwards. These files contain information regarding the status of the SiteScope's groups, monitors, and measurements.

For a reference detailing the XML tags, elements, and attributes included in the integration file that SiteScope forwards to the receiving application, see "XML Tag Reference for Generic Data and Diagnostics Integrations" on page 753.

For user interface details, see "Data Integration Preferences Dialog Box" on page 766.

This section contains the following topics:

Delivery Using HTTP Request

The receiving application must be enabled to receive the data from SiteScope. This means that the application should be able to receive the http request from the SiteScope server and to decipher the XML file when it arrives.

The http request includes the following header:

```
Content-Type: text/xml
```

If you selected to zip the contents of the XML file, then the http request includes the following header:

```
Content-Type: text/xml
Content-Encoding: gzip
```

You select whether to zip the data in the Data Integration Preferences dialog box when creating the integration in SiteScope. If you select to zip the data, your application must be able to unzip the file SiteScope sends.

Time Synchronization

You can synchronize the time of the SiteScope server with your application's server by enabling SiteScope to forward a separate time synchronization XML file. This file is sent in the same way as the data XML and at an interval you select in the **Time synchronization interval** field in the Data Integration Preferences dialog box when creating the integration in SiteScope. If you enter a value in this field, SiteScope forward the date stamp of its server to the application receiving its data at the interval specified. For details on this option, see "Time synchronization interval (minutes)" on page 767. For details on the contents of this XML file, see "Time Synchronization XML" on page 756.

Tasks

How to Configure SiteScope-BSM Integration Preferences for Inaccessible Profiles

This task describes the steps involved in configuring SiteScope as a data collector for BSM when the SiteScope is inaccessible to the BSM, for example when working in HP Software-as-a-Service.

This task includes the following steps:

- "Add a SiteScope profile to BSM" on page 751
- "Specify connection parameters to BSM servers" on page 751
- "Configure SSL for SiteScope-BSM communication" on page 752

1 Add a SiteScope profile to BSM

In BSM, create an empty profile for the SiteScope in SAM Admin's New SiteScope page by selecting **Inaccessible profile**.

For user interface details, see "New SiteScope Page" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

2 Specify connection parameters to BSM servers

In SiteScope, add a new BSM Integration Preference to the Integration Preferences. Enter the values for the BSM integration. When adding the integration, click the **Get Available Profile** button and select the empty profile you created in BSM.

For user interface details, see "BSM Integration Preferences Dialog Box" on page 760.

3 Configure SSL for SiteScope-BSM communication

If you are using a self-signed certificate on the BSM server and want to use that certificate for secure communication with SiteScope, you must perform the appropriate step below:

- For a BSM server that requires SSL, see "How to Connect SiteScope to a BSM Server That Requires SSL" on page 296.
- For a BSM server that requires a client certificate, see "How to Connect SiteScope to a BSM Server That Requires Client Certificate" on page 297.

Reference

XML Tag Reference for Generic Data and Diagnostics Integrations

When SiteScope forwards data for generic data or diagnostics integrations, it does so using the XML files whose elements and attributes are described below. For details on creating the integration, see "Generic Data Integration Overview" on page 749 or "Diagnostics Integration Overview" on page 746.

For user interface details, see "Data Integration Preferences Dialog Box" on page 766 or "Diagnostics Integration Preferences Dialog Box" on page 771.

This section also includes:

- "Data XML Elements and Attributes Table" on page 753
- "Time Synchronization XML" on page 756

Data XML Elements and Attributes Table

Parent Element	Description of Element	Attribute	Description
performance Monitors	The parent element of the XML. Includes all group elements within it.	collectorHost	SiteScope host
		collector	Application collecting the data, which is always SiteScope
group	Represents the SiteScope group and is parent element to group and monitor element	name	Group name as defined by the user
		desc (optional)	Group description if entered for the group
		previousName (optional)	Previous name of the group if existed

Parent Element	Description of Element	Attribute	Description
monitor	Represents the SiteScope monitor and parent element to the counter element	type	Monitor type (as displayed in New Monitor dialog box)
		name	Monitor name as defined by the user
		target	Remote server being monitored
		targetIP	IP address of the remote server being monitored
		time	Time of the measurement
		quality	Status as determined by the monitor's thresholds **Possible values**: ➤ 0 - no data (no thresholds defined) ➤ 1 - informational (good) ➤ 2 - warning ➤ 3 - critical
		previousName (optional)	Previous name of the monitor if existed
		desc (optional)	Monitor description if entered for the monitor
		sourceTemplate Name	Name of the source template if the monitor was created from a template or solution template.
		statusDesc (optional)	Represents monitor's status string that is included only if the **Include additional data** is selected when creating the integration. For details on this option, see "Include additional data" on page 768.

Parent Element	Description of Element	Attribute	Description
counter	Represents the measurements gathered by the monitor	name	Counter name
		value	Counter value
		quality	Status of the counter as determined by the counter's threshold **Possible values**: ➤ 0 - no data (no thresholds defined) ➤ 1 - informational (good) ➤ 2 - warning ➤ 3 - critical
		desc (optional)	Monitor description if entered for the monitor
		status (optional)	If this attribute appears with a value of 0, the counter is not available. This attribute is not sent by SiteScope and not included in the XML if the counter is available. **Possible value**: 0 - counter not available
		units (optional)	Units of measurements for the counter if relevant

Time Synchronization XML

If you enter a value in the **Time synchronization interval** field when creating the data integration, SiteScope sends this XML to synchronize the time of the SiteScope server with that of the receiving application.

Parent Element	Description of Element	Attribute	Attribute Description
performanceMonitors	The parent element of the XML	collectorHost	SiteScope host
		collector	Application collecting the data, which is always SiteScope
timeStamp	Provides the time of the SiteScope server	timestamp	Time stamp, calculated as the seconds since January 1st 1970

 Integration Preferences User Interface

This section includes:

Integration Preferences Page

This page enables you to configure settings when integrating SiteScope with BSM, HPOM, Diagnostics, or other applications.

To access	Select **Preferences** context > **Integration Preferences**
Important information	Only an administrator in SiteScope, or a user granted **Edit integration preferences** permissions can create or make changes to Integration Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	➤ "How to Configure the Integration Between SiteScope and BSM" on page 288 ➤ "How to Configure SiteScope-BSM Integration Preferences for Inaccessible Profiles" on page 751
See also	➤ "Integration Preferences Overview" on page 742 ➤ "Troubleshooting and Limitations" on page 304

User interface elements are described below:

UI Element	Description
	**New Integration.** Creates a new integration in SiteScope. For user interface details, see "Integration Preference Type Dialog Box" on page 759.

UI Element	Description
	**Edit Integration.** Enables editing an existing integration in SiteScope. The Edit Integration dialog box opens according to the integration type selected. ➤ For details on the BSM Integration user interface, see "BSM Integration Preferences Dialog Box" on page 760. ➤ For details on the Data Integration user interface, see "Data Integration Preferences Dialog Box" on page 766. ➤ For details on the Diagnostics Integration user interface, see "Diagnostics Integration Preferences Dialog Box" on page 771. ➤ For details on the HP Operations Manager Integration user interface, see "HP Operations Manager Integration Dialog Box" on page 776.
	**Delete Integration.** Deletes the selected integration from Integration Preferences.
	**Select All.** Selects all listed integrations.
	**Clear Selection.** Clears the selection.
Detach SiteScope	(Available from the shortcut menu only) Detaches SiteScope from LoadRunner integrations. This enables you to delete the current LoadRunner integration from the SiteScope side. When SiteScope is attached, monitors can be defined from the LoadRunner user interface.
Integration Name	Name string assigned to the integration when you create a new Integration Preference.
Integration Description	Description of the integration that was assigned when creating or editing the Integration Preference.

Integration Preference Type Dialog Box

This dialog box enables you to select the type of integration preference you want to configure.

To access	Select **Preferences** context > **Integration Preferences**, and click the **New Integration** button.
Important information	Only an administrator in SiteScope, or a user granted **Edit integration preferences** permissions can create or make changes to Integration Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Configure SiteScope-BSM Integration Preferences for Inaccessible Profiles" on page 751
See also	"Integration Preferences Overview" on page 742

User interface elements are described below:

UI Element	Description
Integration Preference Type	Select an integration preference type: ➤ **BSM Integration.** Use to configure SiteScope as a data collector for BSM. For user interface details, see "BSM Integration Preferences Dialog Box" on page 760. ➤ **Data Integration.** Use to create a generic data integration. For user interface details, see "Data Integration Preferences Dialog Box" on page 766. ➤ **Diagnostics Integration.** Use to create a diagnostics integration. For user interface details, see "Diagnostics Integration Preferences Dialog Box" on page 771. ➤ **HP Operations Manager Integration.** Use to configure SiteScope to send events and report metrics to HPOM and BSM servers. For user interface details, see "HP Operations Manager Integration Dialog Box" on page 776.
Integration Preference Description	Description of the integration preference type.

BSM Integration Preferences Dialog Box

This dialog box enables you to modify BSM integration settings and to create a new BSM integration for a profile that was created in SAM Admin but when the SiteScope was inaccessible.

To access	Select **Preferences** context > **Integration Preferences**. In the Integration Preferences page: ➤ Click the **New Integration** button and select **BSM Integration**, or ➤ Select an existing BSM integration and click the **Edit Integration** button.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit integration preferences** permissions can create or make changes to Integration Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ To secure the connection to BSM (since the BSM user name and password are not used for authentication), it is recommended to configure either Basic Authentication in SiteScope or use two-way SSL. If BSM is configured to use Basic Authentication, the same user name and password entered in the **Authentication user name** and **Authentication password** fields in SiteScope are used for reporting both data and topology to BSM. If BSM is not configured to use Basic Authentication, the credentials sent are ignored. ➤ To enable data to be compressed before being sent from the SiteScope server to BSM, set **_topazCompressDataInGzip=true** in the **<SiteScope root directory>\groups\master.config** file. When enabled, SiteScope monitor (ss_monitor_t) and SiteScope metric (ss_t) samples are compressed in gzip before being sent to BSM (where it is decompressed). Data compression can be used only when SiteScope is reporting to BAC 8.05 or later.

Important information (continued)	➤ By default, data sent from the SiteScope server to BSM is sent uncompressed. For details on enabling data compression, see "Compressing SiteScope Data Sent to BSM" on page 745.
Relevant tasks	➤ "How to Configure the Integration Between SiteScope and BSM" on page 288 ➤ "How to Connect SiteScope to a BSM Server That Requires SSL" on page 296 ➤ "How to Connect SiteScope to a BSM Server That Requires Client Certificate" on page 297 ➤ "How to Configure Topology Reporting" on page 298
See also	➤ "Integration Preferences Overview" on page 742 ➤ "Integration Preferences Page" on page 757 ➤ "Integration Preference Type Dialog Box" on page 759

BSM Integration Main Settings

User interface elements are described below:

UI Element	Description
Business Service Management machine name/IP address	Machine name or IP address of the BSM server to which you want this SiteScope to connect. **Note:** This is a required field.
SiteScope agent machine location	Location of the SiteScope server that you are connecting to BSM. You can specify any value that helps you identify the location of this specific SiteScope server. **Note:** This is a required field.
Disable all logging to Business Service Management	Stops SiteScope from sending data to BSM. This also disables all topology reporting. Clear the check box to enable logging again. **Default value:** Not selected

UI Element	Description
<profile>	SiteScope profile in which BSM stores the data collected by SiteScope. **Note:** The profile must previously have been configured in BSM's SAM Admin.
Get Available Profiles	Displays a list of available profiles. Use this button only if registering the SiteScope to an empty profile (Inaccessible Profile) that was created in SAM Admin.
Business Service Management user name	Username of a BSM administrator-level user.
Business Service Management user password	Password for the specified user.

Web Server Security Settings

User interface elements are described below:

UI Element	Description
Authentication user name	User name to access the server if the BSM server is configured to use basic authentication.
Authentication password	Password to access the server if the BSM server is configured to use basic authentication.
Use SSL (HTTPS protocol)	Select if the BSM server is configured to use the HTTPS protocol. **Default value:** Not selected

Proxy Server Settings

User interface elements are described below:

UI Element	Description
Address	Proxy server address if applicable.
User name	Username for the proxy server.
Password	Password for the specified server.

Topology Reporting Settings

User interface elements are described below:

UI Element	Description
Topology resynchronization time interval (days)	Number of days for SiteScope to synchronize topology data with BSM. The topology information SiteScope reports to BSM is synchronized when SiteScope restarts after this time interval has been reached. **Default value**: 7 days **Minimum value:** 1 day **Note**: All topologies created by SiteScope and stored in RTSM are subjected to the aging process. To prevent aging, see "Aging of CIs in the RTSM" on page 276.
Default topology probe domain	Default domain of the SiteScope topology probe. **Default value**: DefaultDomain **Note:** You must restart SiteScope if you change this setting.
Topology receiver port	Topology receiver port used in BSM. **Default value:** 80 **Note:** You must restart SiteScope if you change this setting.

UI Element	Description
Topology receiver SSL port	Topology receiver SSL port used in BSM. **Default value:** 443 **Note:** You must restart SiteScope if you change this setting.
Topology anti-aging offset (minutes)	Offset from midnight, in minutes, for running the anti-aging process. For details on anti-aging, see "Aging of CIs in the RTSM" on page 276. **Default value:** 0 **Note:** You must restart SiteScope if you change this setting. **Example:** To run anti-aging at 1:30 am, enter an offset of 90.

BSM Preferences Available Operations

User interface elements are described below:

UI Element	Description
Reset	Deletes all the BSM related settings from the SiteScope server and all SiteScope configurations are deleted from BSM. This also sends a message to the applicable BSM 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 BSM. BSM does not enable you to select a previously used connection profile.

UI Element	Description
Re-Synchronize	Forces SiteScope to resend all its configuration data to BSM. This data consists of all the group and monitor definitions. Re-synchronize also forces SiteScope to resend all topology data to BSM.
Hard Re-Synchronize	Forces SiteScope to resend all its configuration data and topology data to BSM. For configuration data, it also deletes the existing monitor and group data from BSM for this SiteScope profile.

Data Integration Preferences Dialog Box

This dialog box enables you to create a new generic data integration or to edit an existing data integration. This can be used to forward SiteScope data to an application for which a direct integration does not exist.

To access	Select **Preferences** context > **Integration Preferences**. In the Integration Preferences page: ➤ Click the **New Integration** button and select **Data Integration**, or ➤ Select an existing Data integration and click the **Edit Integration** button.
Important information	Only an administrator in SiteScope, or a user granted **Edit integration preferences** permissions can create or make changes to Integration Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846.
See also	➤ "Integration Preferences Overview" on page 742 ➤ "Generic Data Integration Overview" on page 749 ➤ "Integration Preferences Page" on page 757 ➤ "Integration Preference Type Dialog Box" on page 759 ➤ "XML Tag Reference for Generic Data and Diagnostics Integrations" on page 753

General Settings

User interface elements are described below:

UI Element	Description
Name	Name by which to identify this integration in the SiteScope interface. **Note:** This is a required field.
Description	Description of the integration. This could include information on the application receiving the data from SiteScope. This description appears only in the Integration Preferences page in SiteScope.

Data Integration Preferences Settings

User interface elements are described below:

UI Element	Description
Receiver URL	URL of the application server to receive the SiteScope data. This must be a full URL including server, port, and path. If secure connection (SSL), then enter https. **Syntax:** http or https://<fully qualified domain name of the receiving server>:<port number receiving data>/<path>
Encoding	Encoding used by the receiving application. **Default value:** UFT-8
Reporting interval (seconds)	Time in seconds between when SiteScope finishes sending data to the next period SiteScope begins sending data. **Default value:** 60 seconds
Time synchronization interval (minutes)	To synchronize between the time of the SiteScope server and the server receiving SiteScope data, SiteScope can periodically report the time that is registered on its server. The receiving server can then synchronize the time of the data samples coming from SiteScope with the time on its own server so that there is no discrepancy between the time of the SiteScope data and the application's own data. Select in minutes how often you want SiteScope to report to the time of the SiteScope server to the server receiving SiteScope data. **Default value:** 10 minutes

UI Element	Description
GZIP compression	Compresses the sample data sent to the receiving server. If the data is compressed, then performance is improved because the time to send data is reduced. Select or clear this field depending on the amount of data being sent and whether the receiving application can handle compressed data. **Default value:** Not selected
Include additional data	If cleared, SiteScope reports the status of the following SiteScope objects: ➤ groups ➤ monitors ➤ counters If selected, the status of these objects are reported along with the status string, which includes the descriptions of each object. **Default value:** Not selected **Tip:** It is recommended not to include additional data as it slows performance, and the status string repeats the status data that is sent by default.
Error on redirect	SiteScope returns an error status if the target URL is redirected. **Default value:** Not selected
Request timeout (seconds)	Timeout, in seconds, until a connection is established with the server. A value of zero means there is no timeout used. **Default value:** 120 seconds
Connection timeout (seconds)	Socket timeout, in seconds, to wait for data. A timeout value of zero means there is no timeout used. **Default value:** 120 seconds
Number of retries	Number of times SiteScope attempts to establish a connection. **Default value:** 3

UI Element	Description
Authentication when requested	SiteScope sends user name and password credentials if requested. If cleared, SiteScope does not forward credentials. **Default value:** Selected
Disable integration	SiteScope does not forward data to the server. The integration preference setting remains. Use when temporarily disabling the integration. **Default value:** Not selected

Web Server Security Settings

User interface elements are described below:

UI Element	Description
Authentication user name	Username to access the server if the server is configured to use basic authentication.
Authentication password	Password to access the server if the server is configured to use basic authentication.

Proxy Server Settings

User interface elements are described below:

UI Element	Description
Address	Proxy server address if applicable.
User name	User name for the proxy server.
Password	Password for the specified server.

Reporting Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	SiteScope uses the tag selected here to determine what data is forwarded to the receiving application. You must select at least one tag for each integration. That same tag must be selected for the groups, subgroups, and monitors whose data you want forwarded to the receiving application. When selecting an integration tag for an object, the tag propagates to that object's children. If you tag a group with this Integration tag, all its subgroups and monitors report their status to the receiving application. **Example:** Create a tag called Integration1 and select it here. For each group, monitor, or both, whose status you want to report to the receiving application, select this tag under the **Search/Filter Tags** setting for the object. **Note**: You can select multiple tags for each integration preference. You can select multiple Integration tags for the objects to be reported.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129. **Tip**: Use the word Integration when creating an Integration tag. Because the Integration tags appear along with all other Search/Filter tags created for the SiteScope, this helps you identify which tag to select for enabling a group or monitor for the integration.

Diagnostics Integration Preferences Dialog Box

This dialog box enables you to create a new integration with HP Diagnostics or to edit an existing Diagnostics integration.

To access	Select **Preferences** context > **Integration Preferences**. In the Integration Preferences page: ➤ Click the **New Integration** button and select **Diagnostics Integration**, or ➤ Select an existing Diagnostics integration and click the **Edit Integration** button.
Important information	Only an administrator in SiteScope, or a user granted **Edit integration preferences** permissions can create or make changes to Integration Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846.
See also	➤ "Diagnostics Integration Overview" on page 746 ➤ "Integration Preferences Page" on page 757 ➤ "Integration Preference Type Dialog Box" on page 759

General Settings

User interface elements are described below:

UI Element	Description
Name	Name by which to identify this integration in the SiteScope interface. **Note:** This is a required field.
Description	Description of the integration. This could include information on the Diagnostics server receiving the data from SiteScope. This description appears only in the Integration Preferences page in SiteScope.

Diagnostics Integration Preferences Settings

User interface elements are described below:

UI Element	Description
Receiver URL	URL of the Diagnostics server to receive the SiteScope data. This must be a full URL including server, port where diagnostics receives data, and path. The path must always include **/metricdata/siteScopeData**. If secure connection (SSL), then enter https. **Syntax:** http or https://<fully qualified domain name of the receiving server>:<port number receiving data>/**metricdata/siteScopeData** **Example**: http://DiagnosticsServer1.hp.net:2006/metricdata/siteScopeData
Encoding	Encoding used by the Diagnostics application. **Default value:** UTF-8
Reporting interval (seconds)	Time in seconds between when SiteScope finishes sending data to the Diagnostics server to the next period SiteScope sends data. This time interval can prevent communication delays between the servers as it is an interval of time when no data is sent. **Default value:** 60 seconds
Time synchronization interval (minutes)	To synchronize between the time of the SiteScope server and the Diagnostics server, SiteScope periodically reports the time that is registered on its server. Diagnostics then synchronizes the time of the data samples coming from SiteScope with the time on its own server so that there is no discrepancy between the time of the SiteScope data and the Diagnostics data. Select in minutes how often you want SiteScope to report to Diagnostics the time of the SiteScope server. **Default value:** 10 minutes

UI Element	Description
GZIP compression	Compresses the sample data sent to the Diagnostics server. If the data is compressed, then performance is improved because the time to send data is reduced. The Diagnostics application can handle compressed data. Select or clear this field depending on the amount of data being sent. **Default value:** Selected
Include additional data	If cleared, SiteScope reports the status of the following SiteScope objects: ➤ groups ➤ monitors ➤ counters If selected, the status of these objects are reported along with the status string, which includes the descriptions of each object. **Default value:** Not selected **Tip:** It is recommended not to include additional data as it slows performance, and the status string repeats the status data that is sent by default.
Error on redirect	SiteScope returns an error status if the target URL is redirected. **Default value:** Not selected
Request timeout (seconds)	Socket timeout, in seconds, which is the timeout for waiting for data. A timeout value of zero is interpreted as an infinite timeout. **Default value:** 120 seconds
Connection timeout (seconds)	Timeout, in seconds, until a connection is established. A value of zero means the timeout is not used. **Default value:** 120 seconds
Number of retries	Number of times SiteScope attempts to establish a connection. **Default value:** 3

UI Element	Description
Authentication when requested	SiteScope sends user name and password credentials if requested. If cleared, SiteScope does not forward credentials. **Default value:** Selected
Disable integration	SiteScope does not forward data to the Diagnostics server. The integration preference settings remain. Use when temporarily disabling the integration. **Default value:** Not selected
Generate UOM XML	Generates a unit of measurement xml file to merge with the **<SiteScope root directory>/conf/integration/data_integration_uom.xml** file. This file enables Diagnostics to read the SiteScope data and apply the appropriate unit of measurement to the data. It is recommended that you click this button when a monitor instance is added that reports data to Diagnostics. If any values were manually changed in the **data_integration_uom.xml** file, those values remain and are not updated by this merge file. This merge file is also generated and updates the xml file on every SiteScope restart. For details, see "Units of Measurements in Diagnostics" on page 746.

Web Server Security Settings

User interface elements are described below:

UI Element	Description
Authentication user name	Username to access the server if the server is configured to use basic authentication.
Authentication password	Password to access the server if the server is configured to use basic authentication.

Proxy Server Settings

User interface elements are described below:

UI Element	Description
Address	Proxy server address if applicable.
User name	Username for the proxy server.
Password	Password for the specified server.

Reporting Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	SiteScope uses the tag selected here to determine what data is forwarded to Diagnostics. You can select more than one tag for each integration. The tag must be selected for the groups, subgroups, and monitors whose data you want forwarded to Diagnostics. When selecting an Integration tag for an object, the tag propagates to that object's children. If you tag a group with this Integration tag, all its subgroups and monitors report their status to Diagnostics. **Example:** Create a tag called Diagnostics_Integration1 and select it here. For each group, monitor, or both, whose status you want to report to Diagnostics, select this tag under the **Search/Filter Tags** setting.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129. **Tip**: Use the word Integration when creating an Integration tag. Because the Integration tags appear along with all other Search/Filter tags created for the SiteScope, this helps you identify which tag to select for enabling a group or monitor for the integration.

HP Operations Manager Integration Dialog Box

This dialog box enables you to configure the HP Operations agent connection settings that enable SiteScope to send common events and metrics data to HPOM and BSM products, and to configure event and metrics integration settings.

To access	Select **Preferences** context > **Integration Preferences**. In the Integration Preferences page: ➤ Click the **New Integration** button and select **HP Operations Manager Integration**, or ➤ Select an existing HPOM integration and click the **Edit Integration** button.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit integration preferences** permissions can create or make changes to Integration Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ Metrics integration with HP Operations Manager can be activated regardless of the connection status between the HP Operations agent and the HPOM/BSM server, since metrics are collected by the agent.
Relevant tasks	➤ "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326 ➤ "How to Enable SiteScope to Report Metrics to the HP Operations Agent" on page 349
See also	➤ "HP Operations Manager Integration Overview" on page 748 ➤ "Sending Events" on page 313 ➤ "Reporting Metrics Using the HP Operations Agent" on page 322 ➤ "Integration Preferences Page" on page 757 ➤ "Integration Preference Type Dialog Box" on page 759

HP Operations Manager Integration Main Settings

User interface elements are described below:

UI Element	Description
Connection Settings	
HP Operations Agent installation path	Path to the HP Operations agent installation on the SiteScope machine. ➤ On Windows platforms, the installation path is automatically resolved from the HP Operations agent **InstallDir** key in the registry, and displayed in this field. The default path is **C:\Program Files\HP\HP BTO Software**. If the key is not found, the field is left empty, and you must manually enter the agent installation path. ➤ On UNIX platforms: SiteScope checks to see if the HP Operations agent is installed in the default **/opt/OV** path. If it is not there, the field is left empty, and you must manually enter the agent installation path. Click the **Resolve Path** button to restore the default installation path found by SiteScope if you manually entered a different path.

UI Element	Description
HP Operations Manager/BSM server	Enter the name or IP address of the HPOM/BSM server to which you want to connect. Click the **Connect** button to connect the agent and the HPOM/BSM host machine. If you are connecting to a BSM distributed environment, enter the BSM Gateway Server name or IP address. If your BSM Gateway Servers are behind a load balancer, enter the name or IP address of the load balancer that is configured for data collectors. For task details, see step 3 in "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326. If there are connection problems, click the **Analyze** button to perform problem analysis and to check the status of the agent and the certificate request. After a connection request is sent, the HPOM/BSM server must grant the certificate request (unless the HPOM/BSM server was configured to accept this client automatically). After the certificate request has been granted on the HPOM/BSM server, click **Install Policies** to install and sign the preconfigured log file policy file on the HP Operations agent. **Note:** You cannot disconnect or change the connection to another HPOM/BSM server from SiteScope after the certificate request has been granted on the HPOM/BSM server. You should contact your HPOM/BSM administrator for assistance.

UI Element	Description
Configuration Settings	
Enable sending events	Enables sending events from SiteScope to the HPOM/BSM server. **Default value:** Not selected
Connect directly to BSM	When the agent is connected to Operations Management in BSM, select to automatically deactivate the node discovery policy if it was installed and enabled on the SiteScope server. When this option is selected: ➤ The **Enable node discovery policy** option is not available, and the node discovery policy is disabled if it was installed and enabled on the SiteScope server. ➤ The **Prefer events over metrics in BSM Service Health (global preference)** option is automatically selected. When this option is cleared: ➤ The **Enable node discovery policy** option is automatically selected. ➤ The **Prefer events over metrics in BSM Service Health (global preference)** option is automatically cleared. **Default value:** Not selected

UI Element	Description
Prefer events over metrics in BSM Service Health (global preference)	The global default preference for influencing BSM's Service Health when both SiteScope events and metrics are reported to Service Health (since indicators for SiteScope events and metrics both affect CIs). This is relevant only when both BSM and HP Operations Manager integrations are active, and are connected to the same BSM server (the BSM server is used instead of the HPOM server). If selected, the **Events** option is set as the default preference for every new monitor created (in **HP Integration Settings** > **BSM Service Health Preferences**). If not selected, **Metrics** is the default preference for reporting data to BSM. For more information on choosing the preference to use, see "Integrating SiteScope with Business Service Management Applications" in *Best Practices for the SiteScope-Business Service Management/Operations Manager Integration* in the SiteScope Help. **Default value:** Not selected (which means metrics data influences Service Health by default) **Note:** ➤ This option is automatically selected if **Connect directly to BSM** is selected. ➤ This setting does not override the preference set for individual monitor instances in **HP Integration Settings** > **BSM Service Health Preferences**.
Enable node discovery policy	SiteScope enables the node discovery policy (if installed) on the SiteScope server. This option is automatically selected when the **Connect directly to BSM** option is cleared. **Default value:** Selected

HP Operations Manager Integration Advanced Settings

User interface elements are described below:

UI Element	Description
Event Integration Settings	
Test message	Checks that the HP Operations agent is connected to the HPOM/BSM server and can send a message. Type a test message to send to the HPOM/BSM server and click the **Send Test Message** button. **Note:** To run the test, the **opcmsg** log policy must be deployed, signed, and installed either manually or after activating the events integration.
Send Test Event	Sends a test event to the HPOM/BSM server.
Severity Mappings Severity mappings control the events severity level of the monitor threshold status in SiteScope when Indicator State is not used. You can customize the default threshold status mappings (below).	
Error	Mapping between the Error status threshold for each monitor instance in SiteScope and the HPOM/BSM server. **Default value:** Critical
Warning	Mapping between the Warning status threshold for each monitor instance in SiteScope and the HPOM/BSM server. **Default value:** Minor
Good	Mapping between the Good status threshold for each monitor instance in SiteScope and the HPOM/BSM server. **Default value:** Normal
Unavailable	Mapping between the Unavailable status threshold for each monitor instance in SiteScope and the HPOM/BSM server. **Default value:** Unknown

UI Element	Description
Use default severity	When selected, the default mappings are sent in: ➤ Events created by a triggered alert. ➤ When SiteScope is not connected to BSM. ➤ In any case where the indicator state and severity value is missing. For example, when using monitors that do not have a defined topology. **Note:** ➤ This option is not available when SiteScope is connected to BSM (and the default global severity mappings cannot be sent). ➤ By default, the Warning state is mapped to Minor (not Warning). **Default value:** Not selected.

HP Operations Manager Metrics Integration

User interface elements are described below:

UI Element	Description
Enable HP Operations Manager metrics integration	Enables SiteScope to report metrics to the HP Operations agent, from which HPOM and the BSM reporting products are able to collect the data. **Note:** You must enable each monitor instance that you want to send data to the HP Operations agent, by selecting **Report metrics to HP Operations agent** in monitor properties (**HP Integration Settings** > **HP Operations Manager Integration Settings**). For details, see "HP Operations Manager Integration Settings" on page 474. **Default value:** Not selected
Enable metrics reporting for specific monitors	Automatically enables reporting metrics for all existing Memory, CPU, Disk Space, and Windows Resources monitors without having to select **Report metrics to HP Operations agent** in the monitor properties for each monitor instance.

25

Log Preferences

This chapter includes:

Concepts

Reference

Concepts

Log Preferences Overview

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

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

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

Note: To create SiteScope Management Reports the monitoring log information for the desired time period of the report must be available on the SiteScope server file system. For details on creating management reports, see "Management Report" on page 1538.

For details on configuring these preferences, see "Log Preferences Page" on page 786.

Reference

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.

Field Name	Example Data	Description
monitorID	10	The ninth field contains the ID of the monitor.
value1, value2, ... value10	(variable)	The tenth through nineteenth fields contain the monitor specific data as described in the Log Columns page. The first variable field (value1) corresponds to the value listed as column 7 in the log files.

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

Log Preferences Page

This page enables you to configure SiteScope Log Preferences. Effective system availability monitoring requires that monitoring data be recorded and stored for a required interval of time. SiteScope Log Preferences controls the accumulation and storage of monitor data.

To access	Select **Preferences** context > **Log Preferences**
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit log preferences** permissions can create or make changes to Log Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ Changes to Log Preferences have an impact only after SiteScope is restarted.
See also	➤ "Log Preferences Overview" on page 784 ➤ "SiteScope Log Database Table Structure" on page 785 ➤ "Troubleshooting and Limitations" on page 790

SiteScope Log File Preferences

User interface elements are described below:

UI Element	Description
Daily logs to keep	Number of days of monitoring data to keep. Once a day, SiteScope deletes any logs older than the specified number of days. **Default value:** 40 **Note:** ➤ The last two logs (today's and yesterday's) are always preserved, regardless of the number of logs or maximum log size specified. ➤ 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 root directory>\logs** directory to estimate the data accumulation rate, and adjust this setting or server resources as necessary.
Maximum size of logs (MB)	Maximum size 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 value:** 0 (the log size is not checked)

Database Logging Preferences

User interface elements are described below:

UI Element	Description
Database connection URL	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 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	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 root directory>\WEB-INF\lib** directory and the path and filename must be entered in this box. **Default value:** sun.jdbc.odbc.JdbcOdbcDriver

UI Element	Description
Database user name	User name to log on to the database. If using Microsoft SQL server, leave this blank and choose Windows Authentication when setting up the ODBC connection. With Windows Authentication, you cannot specify a user name as SiteScope connects using the login account of the SiteScope service. **Note for using Windows Authentication:** The user that is running SiteScope must be able to access the database to which you are connecting. If SiteScope is running under a Local Systems Account, it attempts to connect using the name of the server.
Database password	Password to log on to the database. If using Microsoft SQL server, leave this blank and choose Windows Authentication when creating the ODBC connection. With Windows Authentication, you cannot specify a password as SiteScope connects using the login account of the SiteScope service.
Backup database connection URL	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.

Troubleshooting and Limitations

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

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

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

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

You can also check the HP Software Self-solve knowledge base (http://h20230.www2.hp.com/selfsolve/documents) for other information relating to database logging. To enter the knowledge base, you must log on with your HP Passport ID.

26

Email Preferences

This chapter includes:

Concepts

Reference

Concepts

Email Preferences Overview

You use Email Preferences to configure the settings SiteScope needs to communicate with an external email server. These are the default settings that SiteScope uses to send alerts as email messages.

The Email Preferences page displays the defined custom Email Recipient profiles to send email alert messages to recipients. The Email Recipient profile can be associated with one or more Email alerts by editing the applicable alert definition.

For details on configuring these preferences, see "Email Preferences Page" on page 793.

Reference

Email Preferences User Interface

This section includes:

Email Preferences Page

Email is the default media for sending event alerts when a problem has been detected by SiteScope (in addition to the visual icons and status messages displayed in the SiteScope interface). Use the Email Preferences to indicate the SMTP mail server, recipient addresses, and other settings that SiteScope should use when sending email alerts and other SiteScope messages.

To access	Select **Preferences** context > **Email Preferences**
Important information	Only an administrator in SiteScope, or a user granted **Edit email, pager and SNMP preferences** permissions can create or make changes to Email Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846.
See also	➤ "Email Preferences Overview" on page 792 ➤ "New/Edit Email Recipient Dialog Box" on page 795 ➤ "Email Preferences Default Settings Dialog Box" on page 798

User interface elements are described below:

UI Element	Description
	**New Email Recipient.** Creates a new Email Recipient profile. For user interface details, see "New/Edit Email Recipient Dialog Box" on page 795.
	**Edit Email Recipient.** Enables editing the Email Recipient profile. For user interface details, see "New/Edit Email Recipient Dialog Box" on page 795.
	**Delete Email Recipient.** Deletes the selected Email Recipient profile from Email Preferences.
	**Test Email Recipient.** Tests that you can send a message to the Email address. Enter a message in the Email dialog box, and click **Test**.
	**Select All.** Selects all listed Email Recipient profiles.
	**Clear Selection.** Clears the selection.
Default Settings	Click the arrow next to **Default Settings**, and select an option: ➤ **Edit.** Opens the Email Preferences Default Settings dialog box which enables you to change the default settings displayed in the New Email Recipient dialog box. For details on the settings, see "Email Preferences Default Settings Dialog Box" on page 798. ➤ **Test.** Test that you can send an email to the selected addresses. Select the email recipients you want to test from the list of Available Recipients, or enter email addresses in the **Email addresses** box.
Name	Name string assigned to the setting profile when you create a new Email Recipient.
Description	Description of the setting profile that was assigned when creating or editing the profile.

UI Element	Description
Email	Email address to which the alert is to be sent.
Enabled	Status of the email alert. If the status is **No**, email alerts are stopped from being sent to these email addresses.

New/Edit Email Recipient Dialog Box

This dialog box enables you to create a new Email Recipient profile or edit an existing profile. SiteScope uses Email Recipient profiles for sending email alerts.

To access	Select **Preferences** context > **Email Preferences**. In the Email Preferences page: ➤ Click the **New Email Recipient** button, or ➤ Select an existing Email Recipient profile and click the **Edit Email Recipient** button.
Important information	Only an administrator in SiteScope, or a user granted **Edit email, pager and SNMP preferences** permissions can create or make changes to Email Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846.
See also	➤ "Email Preferences Overview" on page 792 ➤ "Email Preferences Page" on page 793 ➤ "Email Preferences Default Settings Dialog Box" on page 798

Main Settings

User interface elements are described below:

UI Element	Description
Name	Name for the Email Recipient profile definition that is used to identify the profile in the product display.
Description	Description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the , <HR>, and <B> tags to control display format and style. **Note:** HTML code entered here is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans). If malicious HTML code or JavaScript is detected, the entire field is rejected. The following is prohibited HTML content: ➤ Tags: **script**, **object**, **param**, **frame**, **iframe**. ➤ Any tag that contains an attribute starting with **on** is declined. For example, onhover. ➤ Any attribute with **javascript** as its value.
Email to	Email addresses to which you want to send the alert. **Example:** test@mycompany.com You can enter multiple email addresses by separating the email addresses with commas. **Example:** test@mycompany.com, sysadmin@thiscompany.com
Disabled	Stops email alerts from being sent to these email addresses. Use this option to temporarily disable a particular email without editing every alert that contains this email setting.

Advanced Settings

User interface elements are described below:

UI Element	Description
Template	Template defining the email alert settings. Once a setting is defined, a single alert is sent to people and pagers. Use the **ShortMail** template for pagers.
Schedule	Specifies when email settings should be enabled. You may select a more restricted schedule from the names schedules in the drop-down menu. **Default value:** every day, all day

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

Email Preferences Default Settings Dialog Box

This dialog box enables you to configure the default Email Recipient settings.

To access	Select **Preferences** context > **Email Preferences**. In the Email Preferences page, click **Default Settings** > **Edit**.
Important information	Only an administrator in SiteScope, or a user granted **Edit email, pager and SNMP preferences** permissions can create or make changes to Email Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846.
See also	➤ "Email Preferences Overview" on page 792 ➤ "Email Preferences Page" on page 793 ➤ "New/Edit Email Recipient Dialog Box" on page 795

User interface elements are described below:

UI Element	Description
Email server domain name	Domain name of the SMTP mail server that SiteScope should use when sending email messages. **Example:** mail.thiscompany.com If you are unsure of your mail server's domain name, check with your System Administrator.
Administrator email address	Email address to which SiteScope should send status messages. **Example:** sysadmin@thiscompany.com
Daily status	SiteScope sends a brief daily status message to the administrator's email address. This email is scheduled to be generated at 7:07 AM every day. The subject of email sent includes **SiteScope daily status**. The email content includes the number of active monitors and groups, along with a URL link to the applicable SiteScope main page plus the version number of SiteScope installation.

UI Element	Description
SiteScope starts/restarts	SiteScope sends a brief message each time that SiteScope restarts. Restarts may be an indication of a monitor run problem. For more information, see "SiteScope Server Health" on page 1339. **Note:** SiteScope no longer automatically restarts itself once a day.
From email address	Email address used as the From Address for mail generated by SiteScope. Specifying an email address may make it easier to browse and sort email sent by SiteScope. If nothing is entered, the **From email 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 email address entered here must be a valid email address.
Backup email server domain name	Domain name of the SMTP mail server that SiteScope should use whenever the primary mail server cannot be reached. If unsure of backup mail server's domain name, check with the System Administrator. **Example:** gateway.mycompany.com.
Login	Username required by the SMTP server. This user name is used for both the primary and backup mail servers. **Note:** You must restart SiteScope if you change this setting.
Password	Password required by the SNTP server. This password is used for both the primary and backup mail servers. **Note:** You must restart SiteScope if you change this setting.

UI Element	Description
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 **Note:** You must restart SiteScope if you change this setting. **Default value:** none
Timeout (seconds)	Amount 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

27

Pager Preferences

This chapter includes:

Concepts

Reference

Concepts

Pager Preferences Overview

You use Pager Preferences to configure the settings SiteScope needs to communicate with an external electronic paging service. These are the default settings that SiteScope uses to send alerts to an electronic pager.

The Pager Preferences page displays the defined custom Pager Recipient profiles. These profiles can be associated with one or more Pager alerts by editing the applicable alert definition.

You define Pager Recipient profiles in the New/Edit Pager Recipient page. The preferred pager connection option is **Modem to modem connection**. When this connection is used, SiteScope can verify that the message was sent successfully and can receive messages describing any communication problem. The other connection options generally send messages to automated voice response systems using touch tone dialing. The touch tone dialing method is limited to numeric messages and SiteScope cannot confirm that your paging service correctly received the message.

For details on configuring these preferences, see "Pager Preferences Page" on page 803.

Reference

Pager Preferences User Interface

This section includes:

Pager Preferences Page

This page is used to define pager recipient profiles and settings that SiteScope uses for sending Pager alerts to individuals or groups. It lists all the currently defined Pager Recipient profiles. Pager alerts can be used to send an automated notification to system administrators who may not have immediate access to email, or to send alert escalations or notify support personnel who may be away from the office.

To access	Select **Preferences** context > **Pager Preferences**
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit email, pager and SNMP preferences** permissions can create or make changes to Pager Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ You cannot delete a Pager Recipient profile if it is referenced by an alert action. You must change the recipient in the alert before you can delete the profile.
See also	➤ "Pager Preferences Overview" on page 802 ➤ "New/Edit Pager Recipient Dialog Box" on page 805

User interface elements are described below:

UI Element	Description
	**New Pager Recipient.** Creates a new Pager Recipient profile. For user interface details, see "New/Edit Pager Recipient Dialog Box" on page 805.
	**Edit Pager Recipient.** Enable editing the Pager Recipient profile. For user interface details, see "New/Edit Pager Recipient Dialog Box" on page 805.
	**Delete Pager Recipient.** Deletes the selected Pager Recipient profile from Pager Preferences.
	**Test Pager Recipient.** Tests that you can send a message to the pager. Enter a message in the Test Pager dialog box, and click **Test**. You can enter a prefix that can be added to the pager message. If you are sending the message to a numeric pager, do not enter more than 32 digits.
	**Select All.** Selects all listed Pager Recipient profiles.
	**Clear Selection.** Clears the selection.
Default Settings	Click the arrow next to **Default Settings**, and select an option: ➤ **Edit.** Opens the Pager Preferences Default Settings dialog box which enables you to change the default settings displayed in the New Pager Recipient dialog box. For details on the settings, see "New/Edit Pager Recipient Dialog Box" on page 805. ➤ **Test.** Opens the Test Pager dialog box which enables you to test that you can send a message to the default pager. Enter a message in the **Message** box, and click **Test**. You can enter a prefix that can be added to the pager message. If you are sending the message to a numeric pager, do not enter more than 32 digits.

UI Element	Description
Name	Name string assigned to the setting profile when you create a new pager recipient.
Description	Description of the setting profile that was assigned when creating or editing the profile.

New/Edit Pager Recipient Dialog Box

This dialog box enables you to create a new Pager Recipient profile or edit an existing profile. SiteScope uses Pager Recipient profiles for sending Pager alerts.

To access	Select **Preferences** context > **Pager Preferences**. In the Pager Preferences page: ➤ Click the **New Pager Recipient** button, or ➤ Select an existing pager profile and click the **Edit Pager Recipient** button.
Important information	Only an administrator in SiteScope, or a user granted **Edit email, pager and SNMP preferences** permissions can create or make changes to Pager Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846.
See also	➤ "Pager Preferences Overview" on page 802 ➤ "Pager Preferences Page" on page 803

Main Settings

User interface elements are described below:

UI Element	Description
Name	Name string assigned to the setting profile when you create a new pager recipient.
Modem port	Communications port that the modem is connected to on the SiteScope server. For SiteScope on Solaris or Linux, enter the path and device name for the modem. On Microsoft Windows NT/2000 platforms, SiteScope uses COM port numbers for both RS-232C type serial ports as well as for USB modem ports. 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. **Default value:** COM1

UI Element	Description
Connection speed (bit/sec)	Modem speed used for connections to the paging service from the drop-down list. **Default value:** 1200 bit/sec
Pager connection options	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 details of the information required for the selected option, see the table below.

Pager Connection Options

Enter the information required for the selected Pager Connection option:

UI Element	Description
Modem number	Phone number to use for sending alphanumeric pages to the paging service modem.
Modem pin number	Last seven digits of the PIN number for your alphanumeric pager. If you use an alphanumeric paging service, you must enter the phone number to use for sending alphanumeric pages to the paging service modem. This number is provided by your paging service. The paging service sometimes refers to this as the TAP/IXO number.

UI Element	Description
Phone number	Phone number exactly as you would dial it from your telephone, including other numbers you may need, such as a number to get an outside line. You can use dashes to make the number easier to read. Use commas to separate the portions of the phone number. Each comma causes the modem script to pause for a few seconds before dialing the rest of the number. **Example:** If you are dialing your pager from your office, and you have to dial 9 to get an outside line, enter: 9, 555-6789.
Send page command	Page command exactly as you would dial it from your touch tone telephone.
Custom modem command	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.
Disabled	Temporarily disables a particular pager without editing every alert that contains this persons pager. **Default value:** Not selected

Advanced Settings

User interface elements are described below:

UI Element	Description
Schedule	Specifies when pager settings should be enabled. A more restricted schedule can be selected from the drop-down list. **Default value:** every day, all day
Description	Description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the , <HR>, and <B> tags to control display format and style. **Note:** HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. The following is prohibited HTML content: ➤ Tags: **script**, **object**, **param**, **frame**, **iframe**. ➤ Any tag that contains an attribute starting with **on** is declined. For example, onhover. ➤ Any attribute with **javascript** as its value.

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

28

SNMP Preferences

This chapter includes:

Concepts

Reference

Concepts

SNMP Preferences Overview

You use SNMP Preferences to configure the settings SiteScope needs to communicate with an external SNMP host or management console. These are the default SNMP parameters for use with SNMP Trap alerts.

The SNMP Preferences page displays the defined custom SNMP Trap profiles or templates to send traps to hosts. The SNMP Trap profile can be associated with one or more SNMP Trap alerts by editing the applicable alert definition.

For details on configuring these preferences, see "SNMP Preferences Page" on page 813.

Reference

SNMP User Interface

This section includes:

SNMP Preferences Page

This page enables you to define settings that are used by SiteScope SNMP Trap alerts when sending data to management consoles. SiteScope uses the SiteScope SNMP Trap Alert type to integrate with SNMP-based network management systems.

To access	Select **Preferences** context > **SNMP Preferences**
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit email, pager and SNMP preferences** permissions can create or make changes to SNMP Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ You cannot delete an SNMP Trap profile if it is referenced by an alert action. You must change the SNMP Trap in the alert before you can delete the SNMP Trap profile.
See also	➤ "SNMP Preferences Overview" on page 812 ➤ "New/Edit SNMP Trap Dialog Box" on page 815

User interface elements are described below:

UI Element	Description
	**New SNMP Trap.** Creates a new SNMP Trap profile. For user interface details, see "New/Edit SNMP Trap Dialog Box" on page 815.
	**Edit SNMP Trap.** Enables editing the SNMP Trap profile. For user interface details, see "New/Edit SNMP Trap Dialog Box" on page 815.
	**Delete SNMP Trap.** Deletes the selected SNMP Trap profile from SNMP Preferences.
	**Test SNMP Trap.** Tests that you can send a message to the SNMP trap. Enter a message in the Test SNMP Trap dialog box, and click **Test**.
	**Select All.** Selects all listed SNMP Trap profiles.
	**Clear Selection.** Clears the selection.
Default Settings	Click the arrow next to **Default Settings**, and select an option: ➤ **Edit.** Opens the SNMP Trap Preferences Default Settings dialog box which enables you to change the default settings displayed in the New SNMP Trap dialog box. For details on the settings, see "New/Edit SNMP Trap Dialog Box" on page 815. ➤ **Test.** Opens the Test SNMP Trap dialog box which enables you to test that you can send a message to the default SNMP trap. Enter a message in the Test SNMP Trap dialog box, and click **Test**. **Note:** The SNMP Trap test does not send a full trap with all varbinds. It sends the SNMP Trap with the configured trap OID and message only.
Name	Name string assigned to the setting profile when you create a new SNMP trap profile.

UI Element	Description
Description	Description of the setting profile that was assigned when creating or editing the profile.
Host	Domain name or IP address of the machine that receives all SNMP trap messages.
Port	SNMP port to which the trap is sent.

New/Edit SNMP Trap Dialog Box

This dialog box enables you to create a new SNMP Trap profile or edit an existing profile.

To access	Select **Preferences** context > **SNMP Preferences**. In the SNMP Trap Preferences page: ➤ Click the **New SNMP Trap** button or ➤ Select an existing SNMP Trap profile and click the **Edit SNMP Trap** button.
Important information	Only an administrator in SiteScope, or a user granted **Edit email, pager and SNMP preferences** permissions can create or make changes to SNMP Preferences. For details on this topic, see "User Management Preferences Overview" on page 846.
See also	➤ "SNMP Preferences Overview" on page 812 ➤ "SNMP Preferences Page" on page 813

Main Settings

User interface elements are described below:

UI Element	Description
Name	Name string assigned to the setting profile when creating a new SNMP recipient.
Description	Description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the , <HR>, and <B> tags to control display format and style. **Note:** HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. The following is prohibited HTML content: ➤ Tags: **script**, **object**, **param**, **frame**, **iframe**. ➤ Any tag that contains an attribute starting with **on** is declined. For example, onhover. ➤ Any attribute with **javascript** as its value.
Send to host	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.
SNMP port	SNMP port to which the trap is sent. **Default value:** 162
SNMP community	Default SNMP community name used for sending traps. The community string must match the community string used by the SNMP management console. **Default value:** public

UI Element	Description
SNMP trap ID	Select the type of trap to send. There are several predefined ID types for common conditions: ➤ **Generic SNMP trap ID.** Select a generic SNMP type from the drop-down list. ➤ **Enterprise-Specific SNMP trap ID.** To use an enterprise specific SNMP ID type, enter the number of the specific trap type in the box. **Note:** When integrating SiteScope with NNMi, you must select **Enterprise-Specific SNMP trap ID**, and enter **1**. SiteScope sends a different notification ID for each SNMP version: ➤ SNMP V1: .1.3.6.1.4.1.11.15.1.4 ➤ SNMP V2: .1.3.6.1.4.1.11.15.1.4.1
SNMP trap version	Default SNMP protocol version number to use. SNMP V1 and V2c are currently supported. **Default value:** V1
SNMP object ID	Identifies to the console the object that sent the message. ➤ **Preconfigured SNMP object IDs.** Select one of the predefined objects from the drop-down list. ➤ **Other SNMP object ID.** To use another object ID, enter the other object ID in the box. **Note:** When integrating SiteScope with NNMi, select **Preconfigured SNMP object IDs** and choose **HP SiteScope Event** from the list.
Timeout (milliseconds)	Amount of time, in milliseconds, to wait for the SNMP trap requests (including retries) to complete. **Default value:** 500
Retries	Number of times each SNMP trap GET request should be retried before SiteScope considers the request to have failed. **Default value:** 2

UI Element	Description
Add System OID as a prefix to SNMP Trap	Adds the default system OID (1.3.6.1.2.1) as a prefix to all SNMP Trap OIDs. Clear the check box if you do not want to use this prefix. **Default value:** Selected
SNMP source	The SNMP trap source (SiteScope Server or the monitor target server). **Default value:** Monitored Host

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

29

Common Event Mappings

This chapter includes:

Concepts

Tasks

Reference

Concepts

Common Event Mappings Overview

You can configure SiteScope to send events directly to Operations Manager (HPOM) or to Operations Management in BSM. You do this by using Common Event Mappings to create event mapping instances between SiteScope runtime data and the event attribute values that are sent to the HPOM or BSM Gateway Server.

When the event trigger condition is met, the event template is used to map the SiteScope runtime data to the event attributes. These attributes have values that are passed to the event subsystem to create the corresponding event (for example, the template translates the runtime data into an event in HPOM/BSM). The event is then sent to HPOM or BSM.

You can do this by using the default event mapping associated with the monitor or alert, select a different event mapping (if any exist), or create a new event mapping in Common Event Mappings. Alternatively, for alerts, you can use the event mapping template associated with the monitor that triggered the alert. For details on creating event mappings, see "How to Configure Common Event Mappings" on page 822.

For details on the event mapping user interface, see "Event Mapping Page" on page 824.

For details of the event mapping attribute properties, see "SiteScope Alert Template and Event Properties Directory" on page 1451.

For details on configuring SiteScope to report events directly to the Operations Manager server, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326.

Tip: It is recommended to disable any existing event integrations and to configure new integrations when upgrading from versions of SiteScope earlier than 11.00 and versions of BSM earlier than 9.00. Although integrations work after an upgrade, events are used only in the BSM Event Browser.

Tasks

How to Configure Common Event Mappings

This task describes how to use Common Event Mappings to configure event mappings for monitors and alerts. This is the mapping between SiteScope runtime data and the values of event attributes that will be sent.

This task includes the following steps:

- "Prerequisites" on page 822
- "Configure the alerts or monitor instances" on page 823
- "Configure the event mappings for an alert or monitor instance" on page 823
- "Results" on page 823

1 Prerequisites

- To create or make changes to event mappings, you must be an administrator in SiteScope, or a user granted **Edit common event mappings** permissions. For details on user permissions, see "User Management Preferences Overview" on page 846.
- To select an event mapping when configuring an alert or a monitor instance, the HP Operations agent must be installed and connected to an HPOM or BSM server, and event integration must be enabled in the HP Operations Manager Integration dialog box (**Preferences** > **Integration Preferences** > **HP Operations Manager Integration**). For task details, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326.

2 Configure the alerts or monitor instances

You configure the alerts or monitor instances that, where triggered, create the relevant events in the event system.

For task details on creating SiteScope alerts, see "How to Configure an Alert" on page 1443.

For task details on creating monitor instances, see "How to Deploy a Monitor" on page 414.

3 Configure the event mappings for an alert or monitor instance

You configure an event mapping to map an alert or monitor instance to the corresponding event attributes. You can create several mappings for each type of alert or monitor.

For each alert or monitor instance, you can select an existing event mapping, or create a new event mapping in Common Event Mappings. For user interface details, see "New/Edit Event Mapping Dialog Box" on page 826.

Note: The Event mappings list is active only if **Enable sending events** is selected in the **HP Operations Manager Integration Main Settings** pane of the HP Operations Manager Integration dialog box.

---

4 Results

You can view the events corresponding to the triggered alerts or changes in a monitor's metric status in the HPOM Console, or in Operations Management in BSM (if you have an Event Management Foundation license). If Operations Management is not part of your BSM installation, you can view events that affect CI status using a health indicator in Service Health.

Reference

Common Event Mappings User Interface

This section includes:

Event Mapping Page

This page is used to define event mappings and settings. It enables you to configure mappings between SiteScope runtime data and the attribute values of the event to be sent.

To access	Select **Preferences** context > **Common Event Mappings**
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit common event mappings** permissions can create or make changes to Common Event Mappings. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ You cannot delete a common event mapping if it is referenced by a monitor or an alert action. You must change the event mapping referenced by the monitor or alert before you can delete the mapping.
Relevant tasks	➤ "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326 ➤ "How to Configure Common Event Mappings" on page 822
See also	➤ "Common Event Mappings Overview" on page 820 ➤ "New/Edit Event Mapping Dialog Box" on page 826

User interface elements are described below:

UI Element	Description
	**New Event Mapping.** Creates a new event mapping. For user interface details, see "New/Edit Event Mapping Dialog Box" on page 826.
	**Edit Event Mapping.** Enables editing the event mapping. For user interface details, see "New/Edit Event Mapping Dialog Box" on page 826.
	**Delete Event Mapping.** Deletes the selected event mapping from Common Event Mapping list.
	**Select All.** Selects all listed events.
	**Clear Selection.** Clears the selection.
Default Settings	Click the arrow next to **Default Settings**, and select an option: ➤ **Edit Default Monitor Event Mapping.** Opens the Edit Event Mapping dialog box which enables you to change the default monitor event mappings settings. For details on the settings, see "New/Edit Event Mapping Dialog Box" on page 826. ➤ **Edit Default Alert Event Mapping.** Opens the Edit Event Mapping dialog box which enables you to change the default alert event mappings settings. For details on the settings, see "New/Edit Event Mapping Dialog Box" on page 826.
Name	Name string assigned to the setting profile when you create a new event.
Description	Description of the mapping that was assigned when creating or editing the event.

New/Edit Event Mapping Dialog Box

This dialog box enables you to create new common event mappings or edit existing mappings. These are mappings between SiteScope runtime data and the attribute values that are used for sending events.

To access	Select **Preferences** context > **Common Event Mappings**. In the Common Event Mappings page, click the **New Event Mapping** button, or select an existing event and click the **Edit Event Mapping** button. You can also access this dialog box when: ➤ Configuring alerts from the **Alerts** tab > **New/Edit Alert** > **HP Operations Manager Integration Settings** > **Event mapping**. ➤ Configuring a monitor instance from monitor **Properties** tab > **HP Integration Settings** > **HP Operations Manager Integration Settings** > **HP Operations Manager Integration Main Settings.**
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit common event mappings** permissions can create or make changes to Common Event Mappings. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ You cannot delete a common event mapping if it is referenced by a monitor or an alert action. You must change the event mapping referenced by the monitor or alert before you can delete the mapping. ➤ SiteScope might not be able to send events if a long description is entered, or if changes are made to fields in common event mappings that result in field names being too long.
Relevant tasks	➤ "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326 ➤ "How to Configure Common Event Mappings" on page 822
See also	➤ "Common Event Mappings Overview" on page 820 ➤ "Event Mapping Page" on page 824

Main Settings

User interface elements are described below:

UI Element	Description
Name	The name used to identify the common event.
Description	Description of the common event.

Common Event Model Settings - General Tab

User interface elements are described below:

UI Element	Description
General	
Title	Descriptive text describing the occurrence represented by the event. This should include information about what threshold has been crossed (or other trigger conditions), and the current values. **Default value:** ➤ For status change metrics: Metric '<<metric>>' changed status from '<<oldStatus>>' to '<<newStatus>>' ➤ For alerts: Alert '<<alertName>>' was fired on monitor '<<fullMonitorName>>' status change **Tip:** Since the text is typically shown within a single line in the event browser, it is recommended to put the most relevant information at the beginning.
Description	Additional information describing the event. **Default value:** ➤ For status change metrics: Metric '<<metric>>' crossed '<<thresholdCrossed>>' with value '<<metricValue>>' ➤ For alerts: Monitor '<<fullMonitorName>>' changed status from '<<oldStatus>>' to '<<newStatus>>'

UI Element	Description
Severity	Severity of the occurrence related to the event. The severity level can be Unknown, Normal, Warning, Minor, Major, or Critical. **Default value:** <<severity>>. The <<severity>> attribute is replaced by the severity in the **Indicator State and Severity** field in the Threshold Settings for the selected monitor metric.
Category	Value used for organizing or grouping events by monitor type. **Default value:** <<monitorType>> **Examples:** Database, Application, J2EE
Subcategory	Value used for organizing or grouping events that have the same category. **Default value:** ➤ For status change metrics: <<metric>> ➤ For alerts: <<fullMonitorName>> **Example:** Oracle
Log only	If **True** is selected, enables submitting an event that goes directly into the history event browser as a closed event. Such an event goes through the complete event processing, but has its **Life Cycle State** set to close from the beginning. Typical examples are events that result in resetting an indicator to a normal or good state, or an event signaling that a previous problem no longer exists (where the problem was reported in another event). If **True for normal severity** is selected, all messages forwarded from SiteScope to HPOM are sent to the **Acknowledged** message browser (instead of the **Active** message browser) if their severity is normal. This prevents the **Active** message browser becoming unnecessarily cluttered with normal severity messages. **Default value:** False

UI Element	Description
Indicator	Link between the event and the indicator so that information about the indicator can be updated as a result of submitting the event. **Default value:** ➤ For status change metrics: <<etiType>>:<<etiValue>>:<<metricValue>> ➤ For alerts: <<etiType>>:<<etiValue>> **Example of metric status change:** CPU Load:High:90 **Note:** This field is mandatory for updating the indicator. It is not recommended to change the template value of this attribute.
Correlation	
Key	A unique string representing the type of event that occurred. Two events can have the same key if both events represent the same situation in the managed environment. Duplicate events are discarded after the number of duplicate events is increased in the "Number of Duplicates" count. **Default value:** ➤ For status change metrics: <Host>:<Group>:<Monitor>:<Metric>:<etiValue> ➤ For alerts: <<siteScopeHost>>:<<fullgroupid>>:<<monitorName>>:<<alertName>>:<<etiValue>> **Example of metric status change:** labmachine1:OMEventIntegration:CPU Utilization on SiteScope Server:utilization:Good
Submit close key condition	Enables the close key pattern to be evaluated by the event subsystem. If selected, enter the pattern in the **Close key pattern** box below. **Default value:** Selected

UI Element	Description
Close key pattern	(This box is available only if **Submit close key condition** is selected.) Enables the event that is sent to automatically close all the events whose key attribute matches this expression. It is recommended that this field contain the same value as in the **Key** field. **Note:** SiteScope event integration policy always adds "<*>" to the end of your close key pattern. The "<" and ">" signs cannot be used here since that they cannot be interpreted by the log file policy. **Default value:** <<siteScopeHost>>:<<fullgroupid>>:<<monitorName>>:<<metric>> **Example:** labmachine1:OMEventIntegration:CPU Utilization on SiteScope Server:utilization<*>
Advanced Parameters	
CI hint	Information about the CI that is related to the event. This attribute is used for providing hints to enable the event processing to find the correct related CI (RTSM ID of the related CI). **Default value:** <<ciHint>>. The value in this field varies, depending on whether SiteScope is connected to BSM or HPOM. This field is not editable.
Host hint	The target host being monitored by the monitor that triggered the event. The value is translated to the legacy node attribute in HPOM. If the node does not exist in HPOM, the event will be lost. **Default value:** <<targetHost>> **Examples:** ➤ IPv4: 15.15.12.13, ➤ DNS: host1.hp.com

UI Element	Description
Generating source hint	Information about the monitoring application and the corresponding probe/agent that is responsible for creating the event. **Default value:** SiteScope@@<<siteScopeHost>> **Example:** SiteScope@@host1.hp.com
Attributes	
<Attributes list>	Displays the list of available attribute variables. You can add an attribute by dragging it from the **Attributes** list to the selected text box, or select the cell in which to copy the selected attribute, and click Ctrl+I. For a description of the available attribute variables, see "SiteScope Alert Template and Event Properties Directory" on page 1451.

Common Event Model Settings - Custom Attributes Tab

Use this tab to add custom attributes. Custom attributes can be used to provide additional information about the event that is not provided in any of the other common event attributes.

Important information	Make sure that the name of the attribute you are defining is unique and does not already exist in the list of factory attributes. A custom attribute consists of a key and a value (both are strings). The value can be any string and is used by the common event mapping as any other value. **Note:** Only the predefined custom mapping attributes are supported. You cannot change a custom attribute name (cma1-cma5) or add a new one.

User interface elements are described below:

UI Element	Description
	Enables creating a new custom attribute for the event. Each event can have any number of custom attributes. ➤ **New Key.** Adds a new line to the table, enabling you to add a name and value for the attribute. ➤ **Known Key.** Opens a submenu with the known keys as options. You can select the relevant key. A new row opens in the Name/Value table, with the name of the selected key in the Name column. You can then enter the value of the key in the corresponding Value column. **Note:** Only the predefined custom mapping attributes are currently supported. You cannot change a custom attribute name (cma1-cma5) or add a new one.
	**Delete Custom Attribute.** Deletes the selected custom attribute from the table.
Name and Value	Each event can have any number of custom attributes. Custom attributes can be used to provide additional information with the event that is not provided in any of the other common event attributes or that is contained in any of the other attributes. Each custom attribute is a **Name-Value** pair, where you enter the name of the attribute in the **Name** field and the value of the attribute in the **Value** field. This feature may be used when you manage the environment of multiple customers using one instance of the product. The multiple customers might be handled by a custom attribute object. **Example:** Name = "cma1" ; Value = "XYZ Company"

UI Element	Description
Attributes	
<Attributes list>	Displays the list of available attribute variables. You can add an attribute by dragging it from the **Attributes** list to the selected box, or select the cell in which to copy the selected attribute, and click Ctrl+I. For a description of the available attribute variables, see "SiteScope Alert Template and Event Properties Directory" on page 1451.
Service ID	Enables customizing the service name that is sent from SiteScope events to HPOM by entering the value of the monitor service ID. This is useful for relating the SiteScope monitor with the HPOM Service Name. **Default value:** <<monitorServiceId>>

30

Schedule Preferences

This chapter includes:

Concepts

Reference

Concepts

Schedule Preferences Overview

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

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

You may also want to disable certain SiteScope actions based on the schedules of the individuals or groups responsible for the servers and systems being monitored. You use Range Schedules to instruct SiteScope to enable or disable monitors according to time periods that you define.

This section also includes:

➤ "Absolute Schedules" on page 837

➤ "Range Schedules" on page 838

Absolute Schedules

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

Absolute Schedules are inactive until they are explicitly associated with a monitor instance. To associate Absolute Schedules with a monitor, use the **Monitor schedule** field in the **Monitor Run Settings** pane for the monitor that you want to schedule.

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

For details on configuring Absolute Schedule preferences, see "Absolute Schedule Page" on page 839.

Range Schedules

You can use Range Scheduling to specify a time range during which SiteScope either enables or disables particular monitors. If you specify an enabled time range for a monitor (in the **Monitor schedule** field of the **Monitor Run Settings** pane for the specific monitor), SiteScope only runs the monitor during that range. For example, if you create a range of 8AM-9PM, Monday through Friday, any monitors that have that range schedule associated with them are run only during those times.

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

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

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

For details on configuring Range Schedule preferences, see "Range Schedule User Page" on page 841.

Reference

Schedule Preferences User Interface

This section includes:

Absolute Schedule Page

This page is used for customizing the operation of SiteScope monitors and alerts to run only at specific times.

To access	Select **Preferences** context > **Schedule Preferences**. In the Schedule Preferences toolbar, click the **New Schedule** button, and select **New Absolute Schedule**.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit schedule preferences** permissions can create or make changes to Schedule Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ You cannot delete an Absolute Schedule profile if it is referenced by an alert action, report, monitor, or monitor threshold. You must remove the profile from each dependency before you can delete the profile.
See also	"Schedule Preferences Overview" on page 836

General Settings

User interface elements are described below:

UI Element	Description
Name	Name for the Absolute Schedule. The name is used to identify the Absolute Schedule in the product display.
Description	Description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the , <HR>, and <B> tags to control display format and style. **Note:** HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. The following is prohibited HTML content: ➤ Tags: **script**, **object**, **param**, **frame**, **iframe**. ➤ Any tag that contains an attribute starting with **on** is declined. For example, onhover. ➤ Any attribute with **javascript** as its value.

Absolute Schedule Settings

User interface elements are described below:

UI Element	Description
<days of the week>	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

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

Range Schedule User Page

This page is used for customizing the operation of SiteScope monitors and alerts to run only during specific time periods.

To access	Select **Preferences** context > **Schedule Preferences**. In the Schedule Preferences toolbar, click the **New Schedule** button, and select **New Range Schedule**.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit schedule preferences** permissions can create or make changes to Schedule Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ You cannot delete a Range Schedule profile if it is referenced by an alert action, report, monitor, or monitor threshold. You must remove the profile from each dependency before you can delete the profile.
See also	"Schedule Preferences Overview" on page 836

General Settings

User interface elements are described below:

UI Element	Description
Name	Name for the Range Schedule.
Description	Description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the , <HR>, and <B> tags to control display format and style. **Note:** HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. The following is prohibited HTML content: ➤ Tags: **script**, **object**, **param**, **frame**, **iframe**. ➤ Any tag that contains an attribute starting with **on** is declined. For example, onhover. ➤ Any attribute with **javascript** as its value.

Range Schedule Settings

User interface elements are described below:

UI Element	Description
<days of the week>	Days and times the monitor needs to run. Time values for range schedules must be limited to the 24 hour period of a standard day for each day. Select **Enabled** to run monitors during the specified time range only, or **Disabled** to run monitors during all hours of the applicable day, except during the time range. **Note:** The range schedule uses a 24 hour time format only. **Example:** To disable monitors from 6:00 PM on Thursday evening until 8:00 AM the following morning, enter a **From** value of 18 and a **To** value of 24 for Thursday and then enter a **From** value of 0 and a **To** value of 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, in the **From** box enter 2:00,7:00 and in the **To** box enter 3:00,8:00. **Default value:** Enabled (no time values specified). See the table below for more information.

Days of the Week

Enabled Setting (Enabled / Disabled)	Time Range (From /To)	Schedule Effect
Enabled	**From** and **To** time values specified	Monitors are enabled to run only during the **From** and **To** time range.
Enabled	(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.

Enabled Setting (Enabled / Disabled)	Time Range (From /To)	Schedule Effect
Disabled	**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.
Disabled	(no time values specified)	Monitors are disabled during all hours of the applicable day.

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

31

User Management Preferences

This chapter includes:

Concepts

Tasks

Reference

Concepts

User Management Preferences Overview

Note: User Management Preferences are available only to users accessing SiteScope directly and not to users accessing SiteScope using SAM Admin in BSM. For details on how SiteScope permissions interact with BSM, see "Accessing SiteScope and Building Permissions Model" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

You manage SiteScope user accounts from the User Management Preferences page. This page enables you to administer the users that are allowed access to SiteScope. For information on configuring User Management Preferences, see "User Management Preferences Page" on page 864.

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

A user profile limits access to SiteScope to those users that enter a correct user name and password. Optionally, user authentication can be handled by submitting a query to an LDAP database. This enables you to manage users from an external LDAP server by storing authentication information (user names and passwords) for all SiteScope users in a central repository, and using the LDAP server to verify a user's credentials. For more details, see "LDAP Authentication and Authorization" on page 851.

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 creating a SiteScope user profile, see "How to Create a SiteScope User Profile" on page 853.

This section also includes:

User Types and User Role Types

SiteScope provides the following user types and user role types:

User Types:

- **Administrator.** SiteScope provides a single administrator by default. An administrator can view and change anything in SiteScope. It has other special properties as well, such as being allowed to create other users and to change their profiles in the User Management Preferences page. The administrator account cannot be disabled or deleted.
- **Power user (super user).** This is a regular user that has been granted user management permissions. A power user can create, edit, or delete other users, except the administrator. A power user can also edit, but not delete, himself. Both an administrator and a power user can create a power user. There may exist any number of power users. For details about enabling this user type, see "Permissions" on page 873.

- **Regular User.** A regular user cannot create, delete, or edit any user, including itself. It has all the permissions defined for it by the administrator or power user. By default, a regular user is granted all permissions except **Edit user preferences** (under **User Management Preferences**). This limits the user to being able to view their own user properties and the root groups for which they have permissions. A regular user cannot view or edit settings and permissions of other users.

  By default, SiteScope provides an **Integration Viewer** user that is used for drilling down from HPOM events. This is a regular user that has been granted view permissions, and permissions to refresh groups and monitors. For more details, see "Discovery Scripts and the Drill Down User For Viewing HPOM Events" on page 318.

User Role Types: Used to manage groups of SiteScope users when using an external LDAP server.

- **Super User Role.** This is a regular user role that has been granted user management permissions (**Edit user preferences**). Users of this type can create, edit, or delete other users, except the administrator. They can also edit, but not delete, their own user role. Both an administrator and a power user can create a super user role. There may exist any number of super user roles.
- **Regular User Role.** A user of this type cannot create, delete, or edit any user, including itself. It has all the permissions defined for it by the administrator or power user. By default, a regular user role is granted all permissions except **Edit user preferences** (under **User Management Preferences**). This limits the user to being able to view their own user properties and the root groups for which they have permissions. A regular user role cannot view or edit settings and permissions of other users. There may exist any number of regular user roles.

For details about enabling user role types, see "How to Set Up SiteScope to Use LDAP Authentication" on page 855.

For more details about LDAP authentication, see "LDAP Authentication and Authorization" on page 851.

User Permissions

When setting up SiteScope user accounts, the administrator in SiteScope or a power user can configure the permissions required for different users. Permissions limit the areas in SiteScope that a user can access, and control the types of action a user can perform on SiteScope objects, such as groups, monitors, alerts, reports, preferences, remote servers, templates, and Dashboard.

Note: By default, a regular user can view their own user properties and the root groups for which they have permissions only. If a regular user is granted **Edit user preferences** permissions (thereby making the user a power user), the user can edit its own settings and permissions, and create and make changes to the settings and permissions of other users.

User permissions have been extended in SiteScope so that there are specific view, edit, and test permissions for each preference type, and view, edit, and test permissions for remote servers. This enables the administrator or power user to restrict access for selected users to specific preference types and to remote server properties. Where a user does not have view permissions to a specific preference, the tab for that preference is unavailable.

When selecting permissions for an action type, it is important to understand that there are dependency relationships between certain permissions. Edit and test permissions are always dependent on the corresponding view permission. For example, if you select the **Edit remote servers** or **Test remote servers** permission, the **View remote servers** permission is automatically selected. Conversely, if you clear the **View remote servers** permission, the **Edit remote servers** and **Test remote servers** permissions are automatically cleared.

You configure user permissions from the **Permissions** pane of the New/Edit User Profile dialog box. For details on SiteScope user permissions, see "Permissions" on page 873.

Notes and Limitations

- The user preference permissions in SiteScope are not supported in SAM Admin when the SiteScope is reporting to Business Availability Center version 8.00 or earlier.
- When upgrading from versions of SiteScope earlier than 10.10, the permission values are determined as follows:
  - **View <preference type>** permission is selected by default for all preference types (since there was no corresponding preference permission in earlier versions of SiteScope).
  - **Edit <preference type>** permission for all preference types is determined according to the **Edit Preferences** permission in the earlier version of SiteScope.
  - **Test <preference type>** permission for all preference types is determined according to the **Test Preferences** permission in the earlier version of SiteScope.

Notes on User Accounts

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

LDAP Authentication and Authorization

You can choose to configure authentication using the Lightweight Directory Access Protocol (LDAP). This enables you to use an external LDAP server to store authentication information (user names and passwords). SiteScope uses the LDAP server to verify a user's credentials.

Storing information on an LDAP server makes it easier to manage large numbers of users across many SiteScopes. When using LDAP authentication, you can create user role profiles to make managing user permissions more efficient. Instead of assigning access permissions to each user one at a time, you can group users who are assigned the same permissions levels on the same resources to the same user role profile. For details on user roles, see "User Types and User Role Types" on page 847.

In addition to creating and assigning user roles and managing users outside of SiteScope, a SiteScope administrator can also save the list of all LDAP users that have permissions to log on to SiteScope to a CSV file.

For details on enabling LDAP authentication and creating user roles, see "How to Set Up SiteScope to Use LDAP Authentication" on page 855.

For details on other authentication strategies available for logging into SiteScope, see "Authentication Strategies - Overview" on page 928.

Note:

- The audit log contains only the user name (**Displayed Name**), and not the user role or LDAP group (**User role context** or **LDAP context**).
- When a user logs on using LDAP authentication, the user is created for one SiteScope session only. When the session ends, the user is deleted (not saved in persistency).

Silent Authentication

You can also configure authentication via certificates that are stored in the browser or a smart card via client certificate authentication. This is an automatic process that launches SiteScope without having to enter the user login name and password in the SiteScope login page.

When you supply the certificate or enter a smart card, SiteScope takes the unique attributes from the certificate/smart card and uses the LDAP server to verify a user's credentials. When it finds the user, it logs on automatically using the LDAP user credentials.

For details, see "How to Configure Silent Login When Using LDAP Authentication" on page 858.

Tasks

How to Create a SiteScope User Profile

This task describes the steps involved in creating a SiteScope user profile.

This task includes the following steps:

1 Prerequisites

You must be an administrator in SiteScope, or a user granted **Edit user preferences** permissions to be able create or make changes to SiteScope user management settings and permissions. A regular user does not have **Edit user preferences** permissions by default.

For details on user permissions, see "New/Edit User Profile Dialog Box" on page 870.

2 Create an SiteScope user profile

a In the User Management Preferences page, click the arrow next to the **New User** button, and select **New User**.

b In the Main Settings pane, enter the user name, login name and password, and select the groups that can be accessed by this user profile.

For user interface details, see "New/Edit User Profile Dialog Box" on page 870.

3 Assign permissions to the user - optional

Select the permissions granted to this user in the Permissions pane, or use the default permissions (all permissions are granted except **Edit user permissions**).

Click **OK**. The new user profile is added to the User Management Preferences list.

4 Log on to SiteScope

Log on to SiteScope using the new user profile. For details, see "How to Access SiteScope" on page 50.

Note: The SiteScope login password is case sensitive.

SiteScope opens to the Dashboard view and the relevant user permissions are ascribed to the user.

5 Changing a User's Password - optional

You can change a user's password by clicking the **Change Password** link in the SiteScope Login window, and entering the user's user name, current password, and a new password in the Change Password dialog box.

If the new password does not comply with password configuration rules, an error message is displayed and the password is not changed. For password configuration rules, see "Password Requirement Parameters" on page 863.

How to Set Up SiteScope to Use LDAP Authentication

This task describes the steps involved in using LDAP authentication and authorization for logging on to SiteScope.

This task includes the following steps:

1 Prerequisites

- When using LDAP to access SiteScope, users must have a user login and security principal assigned to them on the LDAP server. For details, contact your LDAP server administrator.
- You must be an administrator in SiteScope, or a user granted **Edit user preferences** permissions to be able create or make changes to SiteScope LDAP user management settings and permissions. A regular user does not have **Edit user preferences** permissions by default. For user interface details, see "New/Edit User Profile Dialog Box" on page 870.

2 Enable SiteScope to use LDAP authentication

a In SiteScope, select **Preferences** > **User Management Preferences**, click the arrow next to **Default Settings**, and select **Edit**. The User Management Settings dialog box opens, displaying the LDAP User Management settings. For user interface details, see "User Management Settings Dialog Box" on page 867.

b Select the **Enable LDAP Authentication** check box, and configure the LDAP Authentication settings.

c To test the LDAP connection, click the arrow next to **Default Settings**, and select **Test**. The test status is returned (if the test is successful, the number of LDAP users is displayed).

Note: All users in this LDAP will get viewer permissions without being part of any viewer role if **Enable viewer permissions for all LDAP users** is selected in the User Management Settings dialog box.

---

3 Create an LDAP user role profile

In the User Management Preferences page, click the arrow next to the **New User** button, and select **New User Role**. Enter the user role name, the LDAP security group (context), select the groups that can be accessed by this user role profile, and select the permissions granted to this user role.

For user interface details, see "New/Edit User Role Profile Dialog Box" on page 885.

4 Copy an existing user's permissions to a user role - optional

You can copy an existing SiteScope user's permissions to a new user role. This enables you to assign the same permissions as the user role when creating or editing a user profile.

a In the User Management Preferences page, select a user from which you want to copy permissions to a user role and select **Copy** > **Copy to User Role**.

b In the New User Role Profile dialog box, enter a name and context for the new user role and save it. For user interface details, see "New/Edit User Role Profile Dialog Box" on page 885.

c The permissions of the selected user are copied to the user role, which is added to the User Management Preferences page as a **Regular User Role** or **Super User Role** type (depending on the permissions granted). For user interface details, see "User Management Preferences Page" on page 864.

5 Log off of SiteScope

Click the **LOGOUT** button to log out of SiteScope.

6 Log on to SiteScope

When using LDAP to access SiteScope, users can access SiteScope in the usual ways. For details, see "How to Access SiteScope" on page 50.

Note: SiteScope users still need to have a SiteScope login name and password defined, which they must enter in the SiteScope Login page. (LDAP users have their own LDAP user name and password for logging on to SiteScope.)

---

7 Results

After a user enters their login name and password in the SiteScope Login page (or uses silent login), SiteScope sends a request to LDAP.

If the request returns confirmation of the user and the user's groups match the user role definition, the relevant user role permissions are ascribed to the user, and SiteScope opens to the Dashboard view.

How to Configure Silent Login When Using LDAP Authentication

This task describes the steps involved in configuring silent login to SiteScope via client certificate authentication.

This task includes the following steps:

1 Obtain Client Certificate

Obtain a digital certificate issued by a Certificate Authority. If your organization does not currently have a digital certificate for this purpose, you need to make a request to a Certificate Authority to issue you a certificate.

2 Configure the server certificate properties

Enable silent login by making changes to the configuration files used by the Tomcat server.

a Open the **server.xml** file that is located in the <**SiteScope root directory**>**Tomcat****conf** directory.

b Locate the section of the configuration file that looks like the following:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
-->
```

c Change this section to the following, and enter the required parameters:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->

<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="<Keystore_file_path>"
keystorePass="<Keystore_password>" keystoreType="<Keystore_type>"
keyAlias="<Keystore_alias>" truststoreFile="<truststore_File>"
truststorePass="<truststore_password>" truststoreType="<truststore_type>"
clientAuth="true" />

/>
```

For example:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->

<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="c:\myclientstore.p12"
keystorePass="testing" keystoreType="PKCS12" keyAlias="client"
truststoreFile="..\java\lib\security\cacerts" truststorePass="changeit"
truststoreType="JKS" clientAuth="true" />

/>
```

Note: If there are other HP products installed on the same server as SiteScope, you might need to change port 8443 to another port to avoid conflict.

Tomcat log output is written to the **<SiteScope root dir>\logs\tomcat.log** file. Settings for the log file can be configured from the **<SiteScope root dir>\Tomcat\common\classes\log4j.properties** file.

---

d After setting up SSL access on port 8443, restrict unsecured access to SiteScope by commenting out the **Define a non-SSL HTTP/1.1 Connector on port 8080** section.

3 Import server certificate to SiteScope

Use Certificate Management to import the Certificate Authority certificate. Select **Preferences** > **Certificate Management**, and click the **Import Certificates** button. Select **File** or **Host**, and enter the details of the source server.

For user interface details, see "Certificate Management Page" on page 912.

Note: Only an administrator in SiteScope, or a user with **View/Edit certificates list** permissions can view, add, or make changes to the certificates keystore on the Certificate Management page.

---

4 Configure the LDAP user management settings

a Configure the settings in the LDAP User Management Settings pane. For user interface details, see "User Management Settings Dialog Box" on page 867.

b In the **LDAP User Management Advanced Settings** pane, you can enter a unique attribute for the LDAP user in the **LDAP Active Key authentication identity attribute** box (or you can leave it blank, in which case, the **userPrincipalName** attribute is used).

5 Results

When a user attempts to log on to SiteScope using silent login, SiteScope sends a request to LDAP. If the request returns confirmation of the user and the user's groups match the user role definition, the relevant user role permissions are ascribed to the user, and SiteScope opens to the Dashboard view.

The user name displayed in SiteScope is taken from the user's personal name on the user certificate.

Note:

- The user is created for one SiteScope session only. When the session ends, the user is deleted (not saved in persistency).
- When you log off of SiteScope (by clicking the **LOGOUT** button), the silent login parameter (sis_silent_login_type_default) is displayed in the URL. You must remove this parameter before you can log back on to SiteScope using the refresh action.

Reference

Password Requirement Parameters

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.

User Management User Interface

This section includes:

➤ User Management Preferences Page on page 864

➤ User Management Settings Dialog Box on page 867

➤ New/Edit User Profile Dialog Box on page 870

➤ New/Edit User Role Profile Dialog Box on page 885

➤ Save SiteScope LDAP Users in CSV File Dialog Box on page 887

➤ Select User's Allowed Groups Dialog Box on page 888

User Management Preferences Page

The data provided by SiteScope can be made available to multiple users without granting full administrative privileges to all users. This page enables you to create multiple user accounts that provide different view and edit permissions for different audiences.

To access	Select **Preferences** context > **User Management Preferences**
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit user preferences** permissions can create or make changes to user settings and permissions for the current user or for other users. By default, a regular user does not have **Edit user preferences** permissions, which means that they can view only their own user properties. ➤ The Administrator account is the default account that is active when the product is installed. To create other accounts, you must first edit the Administrator account profile to include a user login name and login password.
Relevant tasks	➤ "How to Create a SiteScope User Profile" on page 853 ➤ "How to Set Up SiteScope to Use LDAP Authentication" on page 855 ➤ "How to Configure Silent Login When Using LDAP Authentication" on page 858
See also	"User Management Preferences Overview" on page 846

User interface elements are described below:

UI Element	Description
	**New.** Click the arrow next to the button, and select: ➤ **New User.** Creates a new user profile. For user interface details, "New/Edit User Profile Dialog Box" on page 870. ➤ **New User Role.** Creates a new user role profile. For user interface details, "New/Edit User Role Profile Dialog Box" on page 885.
	**Edit.** Enables editing the selected user or user role profile. For user interface details, see "New/Edit User Profile Dialog Box" on page 870, and "New/Edit User Role Profile Dialog Box" on page 885.
	**Delete User/User Role.** Deletes the selected user or user role profiles.
	**Copy to User Role.** Enables coping an existing SiteScope user's permissions to a new user role. **Note:** SiteScope users still need to have a user login and a security group assigned to them on the LDAP server. (LDAP users have their own LDAP user name and password for logging on to SiteScope.)
	**Select All.** Selects all listed user and user role profiles.
	**Clear Selection.** Clears the selection.

UI Element	Description
Default Settings	Click the arrow next to **Default Settings**, and select an option: ➤ **Edit.** Opens the User Management Settings dialog box which enables you to change the default LDAP authentication settings. For details on the settings, see "User Management Preferences Page" on page 864. ➤ **Test.** Tests the connection to the LDAP server and the authentication of user. ➤ **Save allowed LDAP users to CSV.** Enables saving a list of all LDAP users that have permissions to log on to SiteScope to a CSV file. For details, see "Save SiteScope LDAP Users in CSV File Dialog Box" on page 887. **Note:** This option is available to SiteScope administrators only
Displayed Name	The title for the user or user role profile that was provided in the **Displayed user name** or **Displayed user role name** box. **Note:** When configuring a user profile, if a user name is not provided, the **Login name** value is used instead.
Login Name/User Role Context	Displays the login name for a user profile, and the LDAP context for a user role.
Login Disabled	Displays the login status. If the check box is cleared, access to SiteScope using the user profile is enabled. If the check box is selected, access to SiteScope with this user profile is not allowed.
User Type	Type of user. For details on the different user types, see "User Types and User Role Types" on page 847.

User Management Settings Dialog Box

This dialog box enables you to configure the default LDAP user management settings.

To access	Select **Preferences** context > **User Management Preferences**. In the User Management Preferences toolbar, select **Default Settings** > **Edit**.
Important information	Only an administrator in SiteScope, or a user granted **Edit user preferences** permissions can create or make changes to LDAP user management settings and permissions. By default, a regular user does not have **Edit user preferences** permissions, which means that they can view only their own user properties.
Relevant tasks	➤ "How to Set Up SiteScope to Use LDAP Authentication" on page 855 ➤ "How to Configure Silent Login When Using LDAP Authentication" on page 858
See also	➤ "User Management Preferences Overview" on page 846 ➤ "User Management Preferences Page" on page 864

LDAP User Management Settings

User interface elements are described below:

UI Element	Description
Enable LDAP authentication	Enables using an external LDAP server for authenticating SiteScope users. **Default value:** Not selected
LDAP server URL	URL of the applicable LDAP server to access the SiteScope service using a centralized LDAP authentication rather than the SiteScope specific password. This way, password authentication for access to SiteScope can be performed by LDAP. **Example:** ldap://ldap.mydomain.com:389.

UI Element	Description
LDAP credentials	Option for providing LDAP server authentication credentials: ➤ **Use user name and password.** Select this option to manually enter user credentials. Enter the user name and password used to access the LDAP server in the **User name** and **Password** box. This enables SiteScope to run search queries in LDAP. ➤ **Select predefined credentials.** Select this option to have SiteScope automatically supply a predefined user name and password for the LDAP server (default option). Select the credential profile to use from the **Credential profile** drop-down list, or click **Add Credentials** and create a new credential profile. For details on how to perform this task, see "How to Configure Credential Preferences" on page 895.
Enable viewer permissions for all LDAP users	Enables viewer permissions for all users in the specified LDAP context, even for users that have not been assigned to a specific SiteScope user role. **Default value:** Not selected
LDAP context	
	**New LDAP context.** Adds a new row at the bottom of the LDAP context table, enabling you to add a new LDAP context.
	**Delete LDAP context.** Deletes the selected LDAP context.
	**Move Up.** Enables you to change the order of the LDAP context list by moving the selected LDAP context up the list.

UI Element	Description
	**Move Down.** Enables you to change the order of the LDAP context list by moving the selected LDAP context down the list.
Context	Displays the LDAP security group for each account added to SiteScope. SiteScope uses the context to search inside of LDAP. **Example:** CN=Operator,OU=Users,OU=Security Groups,DC=ldap,DC=server where CN refers to common name, OU to organizational unit, and DC to domain component.

LDAP User Management Advanced Settings

User interface elements are described below:

UI Element	Description
LDAP user objectClass	Query value used for the LDAP user role name. **Default value:** user
LDAP user identity attribute	Query value used for LDAP users with identical login attributes. **Default value:** sAMAccoutName
LDAP group objectClass	Query value used for the LDAP group (role context). **Default value:** Group
LDAP Active Key authorization identity attribute	LDAP identity attribute for silent login authentication. This field is used with Active Key authentication configuration only. You can enter a unique attribute for identifying the LDAP user, or leave it blank, in which case, the **userPrincipalName** attribute is used. For more information see Silent Login with Active Key, see "Silent Authentication" on page 852.

New/Edit User Profile Dialog Box

This dialog box enables you to create a new user profile or edit an existing profile.

To access	Select **Preferences** context > **User Management Preferences**. In the User Management Preferences page: ➤ Click the arrow next to the **New User** button, and select **New User**, or ➤ Select an existing user profile and click the **Edit** button.
Important information	Only an administrator in SiteScope, or a user granted **Edit user preferences** permissions can create or make changes to user settings and permissions for the current user or for other users. By default, a regular user does not have **Edit user preferences** permissions, which means that they can view only their own user properties.
Relevant tasks	➤ "How to Create a SiteScope User Profile" on page 853 ➤ "How to Set Up SiteScope to Use LDAP Authentication" on page 855
See also	➤ "User Management Preferences Overview" on page 846 ➤ "User Management Preferences Page" on page 864

Main Settings

User interface elements are described below:

UI Element	Description
Displayed user name	Title for the 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 displayed name.

UI Element	Description
Login name	SiteScope login name to access SiteScope using this profile. Alternatively, users can log into SiteScope using LDAP authentication by entering a value in the relevant LDAP cells. **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 on to SiteScope using that login name.
Password	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 on to their user account. For information about password requirements, see "Changing a User's Password - optional" on page 854. All SiteScope passwords are encrypted using 3DES (also known as TDES or Triple Data Encryption Algorithm). Although the TDES key is stored in SiteScope, it cannot be modified. For more information, refer to "Hardening the SiteScope Platform" in the *HP SiteScope Deployment Guide* PDF. **Note:** The SiteScope login password is case sensitive.
Confirm password	Confirmation of 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.

UI Element	Description
LDAP service provider	URL of the applicable LDAP server to access the SiteScope service using a centralized LDAP authentication rather than the SiteScope specific password. This way, password authentication for access to SiteScope can be performed by LDAP. You can specify multiple LDAP service providers by entering either the host name and/or the IP address of each LDAP service provider separated by a semicolon (";"). SiteScope reads the list of LDAP service providers and searches for the available provider from the list.' **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	Security Principal for this user when using LDAP authentication to access the SiteScope service. **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 ("="), semicolon (";"), inverted commas (""). A user name containing invalid characters is unable to log on to SiteScope.
Assign user role	Select to assign the user the same permissions as the user role. The list displays the names of all user roles defined in SiteScope. If you select a user role, the **Login disabled**, **Allowed groups**, and **Permissions** settings are no longer available for selection.
Login disabled	Disables access to SiteScope with this user name and password. Clear the check box to enable access using the user profile.

UI Element	Description
Allowed groups	Displays the list of groups that can be accessed by this user profile. Click the N**ew**  button to open the Select User's Allowed Groups dialog box, and select groups. For user interface details, see "Select User's Allowed Groups Dialog Box" on page 888. To remove user access to a group, select the group and click the **Delete**  button. It is not possible to delete all groups in the list. **Default value:** The SiteScope node is selected to enable access to all groups. **Note:** This field is not visible for an Administrator's settings.

Permissions

Enables you to determine user action permissions. To grant a permission, select the check box to the left of the permission or permission group.

Important information	➤ The Permissions pane is not visible for the administrator's account, since they have full permissions which cannot be changed. ➤ Only an administrator in SiteScope, or a user granted **Edit user preferences** permissions can create or make changes to user settings and permissions for the current user or for other users. ➤ All the permissions in the Permissions pane are selected by default, except for the **Edit user preferences** permissions which must be granted by the SiteScope administrator. ➤ The  icon displayed to the left of a permission group indicates that not all permissions contained within that root group have been selected.
See also	➤ "User Management Preferences Overview" on page 846 ➤ "User Management Preferences Page" on page 864

User interface elements are described below:

UI Element	Description
Groups	
Edit groups	Enables the user to add new groups, rename, copy, or delete existing monitor groups. For details, see "New SiteScope Group Dialog Box" on page 387. **Default value:** Selected
Refresh groups	Enables the user to refresh or force all the monitors within a group to run regardless of their schedule. For details, see "New SiteScope Group Dialog Box" on page 387. **Default value:** Selected
Disable groups	Enables the user to disable groups. For details, see "Enable/Disable Monitors in Group Dialog Box" on page 1321. **Default value:** Selected
Monitors	
Edit monitors	Enables the user to add new monitors, edit existing monitor configurations, or delete monitors. For details, see "Working with SiteScope Monitors" on page 391. **Default value:** Selected
Refresh monitors	Enables the user to refresh or force individual monitors to run regardless of their schedule. For details, see "Working with SiteScope Monitors" on page 391. **Default value:** Selected
Acknowledge monitors	Enables the user to use the Acknowledge function to comment on monitor status on the group detail page. For details, see "Acknowledging Monitor Status" on page 1290. **Default value:** Selected

UI Element	Description
Disable monitors	Enables the user to disable monitors within a group. "Enable/Disable Monitors in Group Dialog Box" on page 1321. **Default value:** Selected
Alerts	
View alerts list	Enables the user to view the list of currently configured alert definitions on the Alert List page. This is a root permission that is required to edit, test, or disable alerts indefinitely. For details, see "SiteScope Alerts Page" on page 1461. **Default value:** Selected
Edit alerts	Enables the user to add a new alert, edit, or delete existing alerts. This option is dependent on the **View alerts list** permission. For details, see "New/Edit Alert Dialog Box" on page 1463. **Note:** Since alert actions are not controlled by alert action preferences permissions, this permission is not dependent on the **View emails, pagers, and SNMP lists** permission. **Default value:** Selected
Test alerts	Enables the user to test an existing alert definition. This option is dependent on the **View alerts list** permission. For details, see "SiteScope Alerts Page" on page 1461. **Default value:** Selected
Disable alerts indefinitely	Enables the user to disable or enable one or more alerts indefinitely. This option is dependent on the **View alerts list** permission. For details, see "New/Edit Alert Dialog Box" on page 1463. **Default value:** Selected
Disable alerts temporarily	Enables the user to disable or enable one or more alerts temporarily. For details, see "New/Edit Alert Dialog Box" on page 1463. **Default value:** Selected

UI Element	Description
Reports	
Generate monitor summary report	Enables the user to use the Browse Monitor form and the Monitor Summary Report. For details, see "Monitor Summary Report" on page 1546. **Default value:** Selected
Generate management report	Enables the user to create a scheduled Management report manually. For details, see "Management Report" on page 1538. **Default value:** Selected
Edit management report	Enables the user to add new report definitions, and edit or delete existing report definitions. For details, see "Management Report" on page 1538. **Default value:** Selected
Generate quick report	Enables the user to create ad hoc SiteScope management reports. For details, see "Quick Report" on page 1542. **Default value:** Selected
Generate alert report	Enables the user to create ad hoc or quick alert reports. For details, see "Alert Report" on page 1548. **Default value:** Selected
Remote Servers	
View remote servers list	Enables the user to view the list of remote servers configured in SiteScope. This is a root permission that is required to edit or test remote servers. For details, see "Remote Server Properties Page" on page 600. If this option is not selected, the following entities are not available: ➤ Remote servers tree and remote servers page in the **Remote Servers** context. ➤ **Add Remote Servers** button in the Monitors context. **Default value:** Selected

UI Element	Description
Edit remote servers	Enables the user to add remote servers to SiteScope and edit remote server settings. This option is dependent on the **View remote servers list** permission. For details, see "Remote Server Properties Page" on page 600. **Default value:** Selected
Test remote servers	Enables the user to test remote server connectivity. This option is dependent on the **View remote servers list** permission. For details, see "Remote Server Properties Page" on page 600. **Default value:** Selected
General Preferences	
View general preferences	Enables the user to view General Preferences. This is a root permission that is required to edit General Preferences. For details, see "General Preferences Page" on page 694. **Default value:** Selected
Edit general preferences	Enables the user to edit General Preferences. This option is dependent on the **View general preferences** permission. For details, see "General Preferences Page" on page 694. **Default value:** Selected
Infrastructure Preferences	
View infrastructure preferences	Enables the user to view Infrastructure Preferences. This is a root permission that is required to edit Infrastructure Preferences. For details, see "Infrastructure Preferences Page" on page 709. **Default value:** Selected
Edit infrastructure preferences	Enables the user to edit Infrastructure Preferences. This option is dependent on the **View infrastructure preferences** permission. For details, see "Infrastructure Preferences Page" on page 709. **Default value:** Selected

UI Element	Description
Integration Preferences	
View integration preferences	Enables the user to view Integration Preferences. This is a root permission that is required to edit Integration Preferences. For details, see "Integration Preferences Page" on page 757. **Default value:** Selected
Edit integration preferences	Enables the user to create or edit Integration Preferences. This option is dependent on the **View integration preferences** permission. For details, see "Integration Preferences Page" on page 757. **Default value:** Selected
Log Preferences	
View log preferences	Enables the user to view Log Preferences. This is a root permission that is required to edit Log Preferences. For details, see "Log Preferences Page" on page 786. **Default value:** Selected
Edit log preferences	Enables the user to edit Log Preferences. This option is dependent on the **View log preferences** permission. For details, see "Log Preferences Page" on page 786. **Default value:** Selected

UI Element	Description
Email, Pager, and SNMP Preferences	
View email, pager and SNMP lists	Enables the user to view the Email, Pager, and SNMP profile lists. This is a root permission that is required to edit or test Email, Pager, and SNMP Preferences. For details, see "Email Preferences Page" on page 793, "Pager Preferences Page" on page 803, and "SNMP Preferences Page" on page 813. **Default value:** Selected
Edit email, pager and SNMP preferences	Enables the user to create or edit Email, Pager, and SNMP Preferences. This option is dependent on the **View email, pager and SNMP lists** permission. For details, see "Email Preferences Page" on page 793, "Pager Preferences Page" on page 803, and "SNMP Preferences Page" on page 813. **Default value:** Selected
Test email, pager and SNMP preferences	Enables the user to test any preference setting for communicating with an external service such as email, pager, or SNMP. This option is dependent on the **View email, pager and SNMP lists** permission. For details, see "Email Preferences Page" on page 793, "Pager Preferences Page" on page 803, and "SNMP Preferences Page" on page 813. **Default value:** Selected

UI Element	Description
Common Event Mappings	
View common event mappings	Enables the user to view Common Event Mappings. This is a root permission that is required to edit Common Event Mappings. For details, see "Common Event Mappings" on page 819. **Default value:** Selected
Edit common event mappings	Enables the user to edit Common Event Mappings. This option is dependent on the **View common event mappings** permission. For details, see "Common Event Mappings" on page 819. **Default value:** Selected
Schedule Preferences	
View schedule list	Enables the user to view Schedule Preferences. This is a root permission that is required to edit Schedule Preferences. For details, see "Schedule Preferences User Interface" on page 839. **Default value:** Selected
Edit schedule preferences	Enables the user to create or edit Schedule Preferences. This option is dependent on the **View schedule list** permission. For details, see "Schedule Preferences User Interface" on page 839. **Default value:** Selected
User Management Preferences	
Edit user preferences	Enables the user to view, edit, or delete user preferences for all other users, except the SiteScope administrator user. A power user cannot delete his/her own account. For users who do not have this permission, the New/Edit User Profile dialog box is displayed as read only, and the settings and root groups for which the current user has permissions are displayed. **Default value:** Not selected

UI Element	Description
Credential Preferences	
View credential list	Enables the user to view Credential Preferences. This is a root permission that is required to edit Credential Preferences. For details, see "Credential Preferences Page" on page 897. If this option is not selected, the following entities are not available: ➤ **Credential Preferences** tab in the Preferences context. ➤ **Add Credentials** button in the Remote Servers and Monitors context. **Default value:** Selected
Edit credential preferences	Enables the user to create or edit Credential Preferences. This option is dependent on the **View credential list** permission. For details, see "Credential Preferences Page" on page 897. **Default value:** Selected
Certificate Management	
View certificates list	Enables the user to view the Certificate Management page. This is a root permission that is required to edit Certificate Management. For details, see "Certificate Management User Interface" on page 912. **Default value:** Selected
Edit certificates list	Enables the user to manage certificates using Certificate Management. This option is dependent on the **View certificates list** permission. For details, see "Certificate Management User Interface" on page 912. **Default value:** Selected

UI Element	Description
Tags	
View tags	Enables the user to view the New/ Edit SiteScope Tag dialog box to see a list of defined tags. This is a root permission that is required to edit tags. For details, see "Search/Filter Tags Page" on page 905. **Default value:** Selected
Edit tags	Enables the user to add, edit, or delete search/filter tags and tag values. This option is dependent on the **View tags** permission. For details, see "Search/Filter Tags Page" on page 905. **Default value:** Selected
Templates	
View templates	Enables the user to view templates that exist in the monitor tree. This is a root permission that is required to edit templates. For details, see "Template Tree" on page 95. **Default value:** Selected
Edit templates	Enables the user to add, edit, and delete templates. This option is dependent on the **View templates** permission. For details, see "Template Tree" on page 95. **Default value:** Selected

UI Element	Description
Dashboard	
Edit favorites	Enables the user to add or delete items in the favorite views list in the SiteScope Dashboard view. For details, see "Save to Dashboard Favorites Dialog Box" on page 1310 and "Delete Dashboard Favorites Dialog Box" on page 1311. **Default value:** Selected
Edit layout	Enables the user to permanently disable fields in the SiteScope Dashboard. For example, if you do not want specific users to see IP addresses of monitored servers, you can permanently hide the Target column in the Dashboard. Users that do not have this permission cannot see the columns that have been disabled. **Default value:** Selected
View monitor history	Enables the user to view the recent history report for a monitor. For details, see "SiteScope Dashboard - Monitor History View" on page 1307. **Default value:** Selected

UI Element	Description
Other	
Use tools	Enables the user to use SiteScope tools in the Tools container to troubleshoot and diagnose monitor configuration problems. For details, see "SiteScope Tools" on page 159. **Default value:** Selected
View logs	Enables the user to view the raw data reported by SiteScope monitors sent by alerts, and other SiteScope logs. For details, see "Using Log Files" on page 1376. **Default value:** Selected
View server statistics	Enables the user to view SiteScope internal data that can be used for analyzing SiteScope server performance, stability, health, and for debugging bottlenecks. For details, see "Using Server Statistics" on page 1372. **Default value:** Selected
Use monitor tools	Enables the user to use SiteScope tools when configuring or editing particular monitor types. If a diagnostic tool is available for a monitor type, the **Tools**  button is enabled in the Dashboard toolbar for that monitor in the group detail page. For details, see "SiteScope Tools" on page 159. **Note:** ➤ Diagnostic tools may expose sensitive system information. ➤ This option is dependent on the **Use tools** permission. **Default value:** Selected

New/Edit User Role Profile Dialog Box

This dialog box enables you to create a new user role profile or edit an existing profile.

To access	Select **Preferences** context > **User Management Preferences**. In the User Management Preferences page: ➤ Click the arrow next to the **New User** button, and select **New User Role**, or ➤ Select an existing user role profile and click the **Edit** button.
Important information	Only an administrator in SiteScope, or a user granted **Edit user preferences** permissions can create or make changes to user settings and permissions for the current user or for other users. By default, a regular user does not have **Edit user preferences** permissions, which means that they can view only their own user properties.
Relevant tasks	"How to Set Up SiteScope to Use LDAP Authentication" on page 855
See also	➤ "User Management Preferences Overview" on page 846 ➤ "User Management Preferences Page" on page 864

Main Settings

User interface elements are described below:

UI Element	Description
Displayed user role name	Title for the use role profile. The title is displayed in the list of users.
User role context	Security group for this user when using LDAP authentication to access the SiteScope service. The user role context is the profile used by SiteScope to search inside of LDAP. **Example:** uid=testuser,ou=TEST,o=this-company.com

UI Element	Description
Login disabled	Disables access to SiteScope with this user name and password. Clear the check box to enable access using the user role profile.
Allowed groups	Displays the list of groups that can be accessed by this user role profile. Click the N**ew**  button to open the Select User's Allowed Groups dialog box, and select groups. For user interface details, see "Select User's Allowed Groups Dialog Box" on page 888. To remove user access to a group, select the group and click the **Delete**  button. It is not possible to delete all groups in the list. **Default value:** The SiteScope node is selected to enable access to all groups. **Note:** This field is not visible for an Administrator's settings.

Permissions

Enables you to determine user role permissions. To grant a permission, select the check box to the left of the permission or permission group.

For the list and explanation of each permission, see "Permissions" on page 873.

Save SiteScope LDAP Users in CSV File Dialog Box

This dialog box enables a SiteScope administrator to save the list of all LDAP users that have permissions to log on to SiteScope to a CSV file.

To access	Select **Preferences** context > **User Management Preferences**. In the User Management Preferences toolbar, select **Default Settings** > **Save allowed LDAP users to CSV**.
Important information	Only an administrator in SiteScope, or a user granted **Edit user preferences** permissions can create or make changes to LDAP user management settings and permissions. By default, a regular user does not have **Edit user preferences** permissions, which means that they can view only their own user properties.
Relevant tasks	"How to Set Up SiteScope to Use LDAP Authentication" on page 855
See also	➤ "User Management Preferences Overview" on page 846 ➤ "User Management Preferences Page" on page 864

User interface elements are described below:

UI Element	Description
File	Name of the CSV file to which to save LDAP users that can log on to SiteScope. This file contain three columns: user role name, LDAP group (role context), and user identical attribute (login).
Save Users	Click the button and select an existing CSV file, or enter the name of a new file to which to save the list of LDAP users.

Select User's Allowed Groups Dialog Box

This dialog box enables you to select the groups, subgroups, or both, that the user can access. Select the box next to individual groups or subgroups to enable access to that group. By default, access is allowed to all groups. To restrict user access to fewer groups, clear the check box for the SiteScope node and then select the individual groups below the SiteScope node to which you want to enable access.

To access	Select **Preferences** context > **User Management Preferences**. In the User Management Preferences page, click the **New User** button, or select an existing user profile and click the **Edit User** button. In the New/Edit User Profile dialog box, click the **New** button in the **Allowed groups** area.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit user preferences** permissions can create or make changes to user settings and permissions for the current user or for other users. By default, a regular user does not have **Edit user preferences** permissions, which means that they can view only their own user properties. ➤ When selected, each of a group's subgroups are also added to the list of allowed groups.
See also	➤ "User Management Preferences Overview" on page 846 ➤ "User Management Preferences Page" on page 864

User interface elements are described below:

UI Element	Description
	Represents an individual SiteScope server. **Default value:** The current container and all child elements are selected.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors). If an alert has been set up for the monitor group or subgroup, the alert symbol is displayed next to the group icon. If a Management report has been set up for the monitor group or subgroup, the report symbol is displayed next to the group icon.
	Represents the collection of available health monitors that are deployed to check proper functioning of SiteScope monitors.

32

Credential Preferences

This chapter includes:

Concepts

Tasks

Reference

Concepts

Credential Preferences Overview

Credential Preferences provide centralized credential management for SiteScope resources. It enables you to input user names and passwords for SiteScope monitors, templates, and remote hosts once as a credential profile, and then have SiteScope automatically supply that information when you configure those resources.

Using Credential Preferences enables you to:

- Create and manage your credentials. You can add, modify, and delete credentials from one central location.
- Update credentials. If credentials for a resource expire or need to be updated, the credential profile can be updated and the changes are applied to all usages of the resource within SiteScope. This saves having to find and manually update all usages of the resource in SiteScope.
- Keep user credentials secure. All passwords stored in Credential Preferences are encrypted. Only an administrator, or a user granted **Edit credential preferences** permissions, can make changes to the credentials.
- Search and replace by credential properties, and replace credentials with other credentials using Global Search and Replace.
- Copy monitors in SiteScope with their credential settings. You can also copy monitors to other SiteScopes when there is more than one SiteScope connected to BSM (only available through SAM Admin). If a credential profile does not exist in the SiteScope to which the monitor is copied, the credential profile is created in that SiteScope.

For task details, see "How to Configure Credential Preferences" on page 895.
For user interface details, see "Credential Preferences Page" on page 897.

This section also includes:

Supported Monitors

You can use Credential Preferences to store credentials for the following monitors:

Monitor Category	Monitor
Application	➤ COM+ Server ➤ SAP CCMS ➤ SAP CCMS Alert ➤ SAP Java Web Application Server ➤ SAP Performance ➤ SAP Work Processes ➤ Siebel Application Server ➤ WebSphere Application Server
Database	➤ Database Counter ➤ DB2 8.x ➤ Oracle Database
Server	➤ IPMI
Web Transaction	➤ URL ➤ URL Content ➤ URL List

Monitoring Credential Profiles

If user credentials expire or change, the monitors using these credentials fail and are in **Error** status. To avoid this situation, you can create a monitor for each credential profile that checks the authentication, and makes all monitors of the monitor type dependent on the test monitor.

For example, you can create an IPMI monitor, IPMI_test_credentials, and manually configure the server login and password. When you configure your IPMI monitors, in the Dependencies pane, enter IPMI_test_credentials in the **Depends on** box and select Available as the **Depends condition**. If the IPMI_test_credentials monitor becomes unavailable for any reason, the IPMI monitors are automatically disabled.

Notes

- Copying credential settings to other SiteScopes is not supported when copying monitors to older versions of SiteScope.
- You cannot delete a credential profile if it is referenced by a monitor or a remote host. You must remove the credential profile from each dependency before you can delete the credential profile.
- If a credential that is used in a template remote host or template monitor has been deleted, you must add the missing credential to Credential Preferences or manually enter credentials for the resource in the template object before deploying the template.

Tasks

How to Configure Credential Preferences

This task describes the steps involved in configuring and managing credentials for SiteScope objects that require user authentication.

This task includes the following steps:

1 Prerequisites

To create or make changes to the credentials, you must be an administrator in SiteScope, or a user granted **Edit credential preferences** permissions.

For details on user permissions, see "Permissions" on page 873.

2 Create a credential profile

Configure a credential profile in Credential Preferences for each SiteScope resource that requires user authentication. For user interface details, see "Credential Preferences Page" on page 897.

For a list of supported monitors, see "Supported Monitors" on page 893.

3 Configure SiteScope resources using credential profiles

When you configure a SiteScope resource that has a credential profile, select the profile in the **Credentials** box in the resource's settings area.

- For user interface details when configuring a monitor, see the Monitor Settings for the specific monitor.
- For user interface details when configuring a remote server, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603, and "New/Edit UNIX Remote Server Dialog Box" on page 610.

4 Update credential profiles

If credentials for a resource change, you can update the credential profile without having to find all usages of the resource and update each resource separately in SiteScope. To change a profile, select the profile in Credential Preferences, click **Edit Credential Profile**, and make the necessary changes.

For user interface details, see "Credential Preferences Page" on page 897.

5 Results

SiteScope authenticates the login and password for the resource using the credentials supplied in Credential Preferences.

Reference

Credential Preferences User Interface

This section includes:

- Credential Preferences Page on page 897
- New/Edit Credential Profile Dialog Box on page 899

Credential Preferences Page

This page provides centralized credential management for SiteScope resources. This enables you to add, update, and delete credentials that are used in configuring SiteScope monitors, templates, and remote hosts.

To access	Select **Preferences** context > **Credential Preferences**
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit credential preferences** permissions, can create or make changes to Credential Preferences. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ You cannot delete a credential profile if it is referenced by a monitor. You must remove the profile from each dependency before you can delete the profile.
Relevant tasks	"How to Configure Credential Preferences" on page 895
See also	➤ "Credential Preferences Overview" on page 892 ➤ "New/Edit Credential Profile Dialog Box" on page 899

User interface elements are described below:

UI Element	Description
	**New Credential Profile.** Creates a new credential profile. For user interface details, see "New/Edit Credential Profile Dialog Box" on page 899.
	**Edit Credential Profile.** Enables editing a credential profile. For user interface details, see "New/Edit Credential Profile Dialog Box" on page 899.
	**Delete Credential Profile.** Deletes the selected credential profile from Credentials Preferences.
	**Select All.** Selects all listed credential profiles.
	**Clear Selection.** Clears the selection.
Name	Name string assigned to the setting profile when you create a new credential profile.
Login	User name to access the resource using this credential profile.
Description	Description of the setting profile that was assigned when creating or editing the credential profile.

New/Edit Credential Profile Dialog Box

This dialog box enables you to create a new credential profile or edit an existing profile. You use credential profiles for storing and managing authentication credentials for SiteScope resources.

To access	Select **Preferences** context > **Credential Preferences**. In the Credential Preferences page: ➤ Click the **New Credential Profile** button, or ➤ Select an existing credential profile and click **Edit Credential Profile** button.
Important information	➤ Only an administrator in SiteScope, or a user granted **Edit credential preferences** permissions can create or make changes to Credential Preferences. ➤ This page opens in view mode or edit mode depending on your user permissions. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Configure Credential Preferences" on page 895
See also	➤ "Credential Preferences Overview" on page 892 ➤ "Credential Preferences Page" on page 897

Main Settings

User interface elements are described below:

UI Element	Description
Name	Descriptive name for the credential profile. **Maximum length:** 50 characters
Domain	Domain for the credential. During the connection, the domain is added to the login in the format: <domain>\<login>.
Login	User name to access the resource using this credential profile.

UI Element	Description
Password	Password to access the resource using this credential profile. 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	Confirmation of the password entered in the **Password** box. This is used when creating a new credential or changing the password of an existing credential.

Advanced Settings

User interface elements are described below:

UI Element	Description
Description	Description for the setting profile, which appears only when editing or viewing its properties. You can include HTML tags such as the , <HR>, and <B> tags to control display format and style. **Note:** HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. The following is prohibited HTML content: ➤ Tags: **script**, **object**, **param**, **frame**, **iframe**. ➤ Any tag that contains an attribute starting with **on** is declined. For example, onhover. ➤ Any attribute with **javascript** as its value.

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

33

Search/Filter Tags

This chapter includes:

Concepts

Reference

Concepts

Search/Filter Tags Overview

You use Search/Filter Tag Preferences to manage the Search/Filter Tags defined in SiteScope. These tags can be assigned to items in the context tree or preference profiles, and they are used as objects for a filter.

The Search/Filter Tag Preferences page displays the list of Search/Filter Tags. You can add, edit, or delete Search/Filter Tags from this page.

For details on configuring these preferences, see "Search/Filter Tags Page" on page 905.

Reference

Search/Filter Tags Page

This page enables you to manage the Search/Filter tags defined in SiteScope. You can assign tags to one or more items in the context trees and preference profiles, and then use the tags as an object for a filter.

To access	Select **Preferences** context > **Search/Filter Tags**
Important information	➤ You cannot delete a Search/Filter tag or tag value if it is referenced by a SiteScope object. You must remove the tag or tag value from all SiteScope objects before you can delete it. ➤ Tags can also be used in alert templates using the <tag> attribute. For details, see "SiteScope Alert Template and Event Properties Directory" on page 1451.
Relevant tasks	"How to Create and Define a New Search/Filter Tag" on page 119
See also	➤ "Working with Search/Filter Tags" on page 118 ➤ "Search/Filter Tags Overview" on page 904

User interface elements are described below:

UI Element	Description
	**New Tag.** Creates a new search/filter tag. For user interface details, see "New/Edit Tag Dialog Box" on page 129.
	**Edit Tag.** Enable editing a search/filter tag. For user interface details, see "New/Edit Tag Dialog Box" on page 129.
	**Delete Tags.** Deletes the selected tag from Search/Filter Tag Preferences.

UI Element	Description
	**Select All.** Selects all listed search/filter tags.
	**Clear Selection.** Clears the selection.
Name	Name string assigned to the setting profile when you create a new search/filter tag.
Description	Description of the setting profile that was assigned when creating or editing the search/filter tag.

34

Certificate Management

This chapter includes:

Concepts

Tasks

Reference

Concepts

Certificate Management Overview

When monitoring a remote server, if the target server uses a self-signed certificate, the certificate must be added to a trusted keystore. If you are monitoring a URL, a WebSphere Application Server, or a VMware-based server using a secure connection, you can manage self-signed certificates from the Certificate Management page.

Benefits of using Certificate Management include:

- Certificates do not need to be managed using the standard JVM tools (keytool). This avoids the requirement for a desktop/shell session to the SiteScope machine.
- Provides visual keystore management (add and remove certificates) and enables dynamic keystore reload, without having to restart SiteScope after each certificate change operation.

Note:

- Only an administrator in SiteScope, or a user with **View/Edit certificates list** permissions can view, add, or make changes to the certificates keystore on the Certificate Management page.
- Monitors are bound to the keystores that they are using. For URL, WebSphere Application Server, and VMware Performance monitors, the following keystore is used: **<SiteScope root directory>\java\lib\security\cacerts**. Other keystores are ignored.
- You can still import certificates using the keytool method if preferred. For details on manually importing certificates, see the documentation for the specific monitor type.
- If you use a self-generated Certificate Authority (CA) certificate to sign all the server certificates, you only need to import the CA certificate once.

For details on importing certificates using Certificate Management, see "How to Import Server Certificates Using Certificate Management" on page 910.

For user interface details, see "Certificate Management Page" on page 912.

Tasks

How to Import Server Certificates Using Certificate Management

This task describes the steps involved in importing self-signed certificates using Certificate Management.

This task includes the following steps:

- "Prerequisites" on page 910
- "Import the server certificate" on page 911
- "Configure the monitor properties" on page 911

1 Prerequisites

- Certificate Management can be used to import server certificates that are required when configuring secure connections for the following monitors only: URL, URL Content, URL List, URL Sequence, VMware Performance, VMware Host, and WebSphere Application Server.
- Only an administrator in SiteScope, or a user with **View/Edit certificates list** permissions can view, add, or make changes to the certificates keystore on the Certificate Management page. For details on user permissions, see "Permissions" on page 873.

2 Import the server certificate

If the Web server on which you are monitoring has an https:// prefix, it is a secure, encrypted connection, and you need to import the server certificate.

a Select **Preferences** > **Certificate Management**, and click the **Import Certificates** button. Select **File** or **Host**, and enter the details of the source server. For user interface details, see "Import Certificates Dialog Box" on page 914.

b From the Loaded Certificates table, select the server certificates to import and click **Import**. The imported certificates are listed on the Certificate Management page. For user interface details, see "Certificate Management Page" on page 912.

3 Configure the monitor properties

After importing the required server certificates, you can create a monitor with a secured connection.

Reference

Certificate Management User Interface

This section includes:

Certificate Management Page

This page is used for managing certificates used with SiteScope URL, URL Content, URL List, URL Sequence, VMware Performance, or WebSphere Application Server monitors. The Certificate Management page enables you to add, remove, and refresh keystore contents.

To access	Select **Preferences** context > **Certificate Management**.
Important information	➤ Only an administrator in SiteScope, or a user with **View/Edit certificates list** permissions can view, add, or make changes to the certificates keystore on the Certificate Management page. ➤ You can change the sort order in the columns by clicking the arrow in the column title. A small down or up arrow is displayed indicating the column is sorted in ascending or descending order.
Relevant tasks	"How to Import Server Certificates Using Certificate Management" on page 910
See also	"Certificate Management Overview" on page 908

User interface elements are described below:

UI Element	Description
	**Import Certificates.** Opens the Import Certificates dialog box and add certificates to the Certificate Management keystore list. For user interface details, see "Import Certificates Dialog Box" on page 914.
	**Remove Certificates.** Deletes the selected certificates from the Certificate Management keystore list.
	**Reload Certificate List.** Reloads the keystore certificates from the **<SiteScope root directory>\java\lib\security\cacerts** files on the remote server. This enables you to manually reload keystore changes without having to restart SiteScope.
	**Select All.** Selects all listed certificates.
	**Clear Selection.** Clears the selection.
<certificates>	Lists the server certificates that have been imported. Double-click a certificate to open the Certificate Details dialog box and display the certificate's properties and values. For user interface details, see "Certificate Details Dialog Box" on page 916.
Alias	Certificate alias name. **Note:** Alias names of imported certificates cannot be modified (they can be modified only during the import certificate step).
Issuer	Name of the certificate issuer.
Valid Until	Time and date until which the certificate is valid.
Version	Certificate version number.

Import Certificates Dialog Box

This dialog box is used for adding certificates used with SiteScope URL, WebSphere Application, and VMware Performance monitors to the Certificate Management list keystore. The Certificate Management page enables you to add, remove, and refresh keystore contents.

To access	Select **Preferences** context > **Certificate Management**. Click the **Import Certificates** button.
Important information	➤ Only an administrator in SiteScope, or a user with **View/Edit certificates list** permissions can view, add, or make changes to the certificates keystore on the Certificate Management page. ➤ You can change the sort order in the columns by clicking the arrow in the column title. A small down or up arrow is displayed indicating the column is sorted in ascending or descending order.
Relevant tasks	"How to Import Server Certificates Using Certificate Management" on page 910
See also	"Certificate Management Overview" on page 908

User interface elements are described below:

UI Element	Description
Source Selection	
File	Adds certificates from a file. Click the **Select** button, navigate to the file from which you want to import certificates, and click **Open**. Add the required certificates to the Certificate Management list.
Host	Adds certificates from a host server. Enter the real IP address or host name of the monitored server.
Port	Port number of the host machine (available only if the **Host** option is selected). **Default Port value:** 443

UI Element	Description
Load	Loads certificates for the machine specified in the **Host** field. The certificates are displayed in the Loaded Certificates table.
Loaded Certificates	
	**Select All.** Selects all listed certificates.
	**Clear Selection.** Clears the selection.
Alias	Certificate alias name. You can modify a certificate alias during the import certificate step by entering a new alias in the **Alias** column. **Note:** An alias name cannot be modified after the certificate has been imported.
Issuer	Name of the certificate issuer.
Valid Until	Time and date until which the certificate is valid.
Version	Certificate version number.
Import	Select the certificates to import from the Loaded Certificates table, and click **Import**. The imported certificates are displayed in the Certificate Management page.

Certificate Details Dialog Box

This dialog box displays properties and values for the selected server certificate.

To access	Select **Preferences** context > **Certificate Management**. Double-click a certificate in the Certificate Management page.
Important information	Only an administrator in SiteScope, or a user with **View/Edit certificates list** permissions can view, add, or make changes to the certificates keystore on the Certificate Management page.
See also	"Certificate Management Overview" on page 908

User interface elements are described below:

UI Element	Description
Alias	Certificate alias name.
Certificate Properties	
Fingerprint	The certificate's fingerprint.
Type	The certificate type.
Version	Version number of the certificate.
Issuer principal	Name of the certificate issuer.
Serial number	Serial number of the certificate.
Signature algorithm name	Name of the signature algorithm of the certificate.
Valid from	Time and date from which the certificate is valid.
Valid until	Time and date until which the certificate is valid.

35

Using SiteScope in an Internationalization (I18N) Environment

This chapter includes:

Concepts

Tasks

Reference

Concepts

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
French	French [fr]
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 "How to View SiteScope User Interface in a Specific Language" on page 922.

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

Notes and Limitations

- There is no language pack installation. All translated languages are integrated into SiteScope Multi-lingual User interface (MLU).
- Data stays in the language it was entered in, even if the language of the Web browser changes. Changing the language of the Web browser on your local machine does not change the language of monitor definitions and configurations.
- Names of entities included with the SiteScope installation, such as template examples, solution templates, views, and health monitors, are in English only.
- French is not supported in the installation wizard user interface.
- SiteScope Help can be viewed in Japanese if that is the language that you have selected for the user interface. When you select **Help on this page** or **SiteScope Help**, it is displayed in Japanese. To enable this function, you must install a software patch. Contact HP Software Support (http://www.hp.com/go/hpsoftwaresupport) for further information.
- Other links in the Help drop-down list, such as **Troubleshooting & Knowledge Base**, **HP Software Support**, and **HP Software Web Site**, are also displayed in the user interface language you selected.

Tasks

How to Configure SiteScope for a Non-English Locale

This task describes the steps involved in configuring SiteScope for a non-English locale.

This task includes the following steps:

1 Change the locale version setting

In the monitor tree, select **Preferences** > **General Preferences**. In the **Main Panel**, select **International version**, and click **Save**. Restart SiteScope. This enables SiteScope to work with multiple character sets.

For user interface details, see "International version" on page 697.

2 Set new locale time and data settings

You can set a new locale time and data settings for SiteScope.

a Open <**SiteScope root directory**>**groups****master.config** in a text editor.

b Find the entry _localeCountry=, and assign it an uppercase 2-character ISO-3166 country code. For example: _localeCountry=US. A list of country codes is available at http://www.chemie.fu-berlin.de/diverse/doc/ISO_3166.html.

c Find the entry _localeLanguage=, and assign it a lowercase 2-character ISO-639 language code. For example: _localeLanguage=en. A list of language codes is available at http://www.ics.uci.edu/pub/ietf/http/related/iso639.txt.

d Save the file and restart SiteScope.

3 View SiteScope user interface in a specific language

Select a language preference for viewing the SiteScope user interface.

For details on how to perform this task, see "How to View SiteScope User Interface in a Specific Language" on page 922.

4 Results

SiteScope is configured to work with multiple foreign character sets, the time and data settings are displayed in a locale-specific format, and the user interface is displayed in a foreign language.

How to View SiteScope User Interface in a Specific Language

This task describes how to select a language preference for viewing the SiteScope user interface.

Note: For a list of supported languages, see "Multi-Lingual User (MLU) Interface Support" on page 918.

---

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

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

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

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

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

   b. Select 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 and to close the Language dialog box.

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

Reference

Monitors Supported for Internationalization

The following monitors are supported for internationalization. Monitors that have been certified are indicated by an asterisk (*).

Monitors Supported for Windows Operating Systems

- *CPU Monitor
- Database Counter Monitor
- *Database Query Monitor
- *Disk Space Monitor
- *DNS Monitor
- *e-Business Transaction Monitor
- *File Monitor
- *FTP Monitor
- Link Check Transaction Monitor
- *Log File Monitor
- *Memory Monitor
- Microsoft IIS Server Monitor
- Microsoft SQL Server Monitor
- Microsoft Windows Event Log Monitor
- Microsoft Windows Performance Counter Monitor
- Microsoft Windows Resources Monitor
- Oracle 9i Application Server Monitor
- *Oracle 10g Application Server Monitor
- *Oracle Database Monitor

- *Ping Monitor
- *Port Monitor
- *Script Monitor
- *Service Monitor
- SNMP Monitor
- SNMP Trap Monitor
- UDDI Monitor
- *URL Monitor
- URL Content Monitor
- URL List Monitor
- URL Sequence Monitor
- *VMware Performance Monitor
- Web Script Monitor

Monitors Supported for UNIX Operating Systems

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

Troubleshooting and Limitations

This section contains troubleshooting and limitations for the following issues relating to working with SiteScope in an internationalization environment.

General Limitations for Using SiteScope in an I18N Environment

- User name, password, and URLs must be in English characters.
- 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 "How to Configure SiteScope for a Non-English Locale" on page 920.
- When deploying the Web Script Monitor, script names and transaction names must also be in English characters.
- Script monitor on Redhat ES4 does not support parameters in any language other than English.
- SiteScope always uses "en_US" locale for parsing dates retrieved from remote UNIX machines (for example, during a File monitor run). If the UNIX machine's default locale is different from en_US, in the definition of the UNIX remote for this machine, the **Initialize Shell Environment** field must contain "LANG=C; export LANG".
- SiteScope Management reports do not support non-English labels.

Database Environment Issues

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

Troubleshooting Remote UNIX Servers Not Configured For an English Locale

- The File Monitor and Directory Monitor may fail when using UNIX remote servers that are not configured by default for an English locale or language. **Workaround:** Add "LANG=C; export LANG" to the **Initialize Shell Environment** property of the problematic UNIX remote server.

36

Set Up the Authentication Strategy for Logging into SiteScope

This chapter includes:

Concepts

Tasks

Concepts

Authentication Strategies - Overview

SiteScope authentication is based on a concept of authentication strategies. Each strategy handles authentication against a specific authentication service. Only one authentication service can be configured with SiteScope at any given time.

The default authentication strategy for logging on to SiteScope is the SiteScope internal authentication service. You enter your SiteScope user name and password from the login page, and your credentials are stored and verified by SiteScope.

SiteScope supports Single Sign-On (SSO), a method of access control that enables a user to log on once and gain access to the resources of multiple software systems without being prompted to log on again. The applications inside the configured group of software systems trust the authentication, and there is no need for further authentication when moving from one application to another.

SiteScope supports the following SSO authentication strategies:

- **Lightweight Single Sign-On (LW-SSO)**. This is the default single sign-on authentication strategy for SiteScope. LW-SSO is embedded in SiteScope and does not require an external machine for authentication. After installing SiteScope, you should immediately change the default passphrase string for all HP software applications integrated using LW-SSO. For details on changing the default SSO value in SiteScope, see "Change the Lightweight Single Sign-On string in SiteScope" on page 930.

  For limitations, security warnings, and general reference on using LW-SSO, see "Lightweight Single Sign-On Authentication (LW-SSO) – General Reference" on page 931.

➤ **Lightweight Directory Access Protocol (LDAP)**. You can configure authentication using the Lightweight Directory Access Protocol (LDAP). This enables you to use an external LDAP server to store authentication information (user names and passwords). SiteScope uses the LDAP server to verify a user's credentials. You enable and disable LDAP authentication from User Management Preferences. For details, see "LDAP Authentication and Authorization" on page 851.

Tasks

How to Set Up the Authentication Strategy for Logging on to SiteScope

The following steps describe how to set up authentication strategies for logging on to SiteScope.

➤ "Change the Lightweight Single Sign-On string in SiteScope" on page 930

➤ "Enable SiteScope to use LDAP authentication - optional" on page 930

Change the Lightweight Single Sign-On string in SiteScope

After installing SiteScope, you should immediately change the default passphrase string for all HP software applications integrated using LW-SSO.

➤ In applications other than SiteScope, locate the **lwssofmconf.xml** file and change the value directly in that file.

➤ In SiteScope, you can do this directly in the **<SiteScope root directory>\conf\lwsso\lwssofmconf.xml** file (only before the first time the service is loaded). You can also change the value in **Preferences** > **General Preferences** > **LW SSO Settings** > **LW SSO Init String**.

Enable SiteScope to use LDAP authentication - optional

For concept details, see see "LDAP Authentication and Authorization" on page 851.

For task details, see see "How to Set Up SiteScope to Use LDAP Authentication" on page 855.

37

Lightweight Single Sign-On Authentication (LW-SSO) – General Reference

This chapter includes:

Concepts

Reference

Concepts

LW-SSO Authentication Overview

LW-SSO is a method of access control that enables a user to log on once and gain access to the resources of multiple software systems without being prompted to log on again. The applications inside the configured group of software systems trust the authentication, and there is no need for further authentication when moving from one application to another.

The information in this section applies to LW-SSO version 2.4.

This section includes the following topics:

LW-SSO Token Expiration

The LW-SSO Token's expiration value determines the application's session validity. Therefore, its expiration value should be at least the same value as that of the application session expiration value.

Recommended Configuration of the LW-SSO Token Expiration

Each application using LW-SSO should configure token expiration. The recommended value is 60 minutes. For an application that does not require a high level of security, it is possible to configure a value of 300 minutes.

GMT Time

All applications participating in an LW-SSO integration must use the same GMT time with a maximum difference of 15 minutes.

Multi-domain Functionality

Multi-domain functionality requires that all applications participating in LW-SSO integration configure the trustedHosts settings (or the **protectedDomains** settings), if they are required to integrate with applications in different DNS domains. In addition, they must also add the correct domain in the **lwsso** element of the configuration.

Get SecurityToken for URL Functionality

To receive information sent as a **SecurityToken for URL** from other applications, the host application should configure the correct domain in the **lwsso** element of the configuration.

Reference

LW-SSO System Requirements

The following table lists LW-SSO configuration requirements:

Application	Version	Comments
Java	1.5 and higher	
HTTP Sevlets API	2.1 and higher	
Internet Explorer	6.0 and higher	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality
FireFox	2.0 and higher	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality
JBoss Authentications	JBoss 4.0.3 JBoss 4.3.0	
Tomcat Authentications	Standalone Tomcat 6.0.29	
Acegi Authentications	Acegi 0.9.0 Acegi 1.0.4	
Spring Security Authentication	Spring Security 2.0.4	
Web Services Engines	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

LW-SSO Security Warnings

This section describes security warnings that are relevant to the LW-SSO configuration:

- **Confidential InitString parameter in LW-SSO.** LW-SSO uses Symmetric Encryption to validate and create a LW-SSO token. The **initString** parameter within the configuration is used for initialization of the secret key. An application creates a token, and each application using the same initString parameter validates the token.

Caution:

- It is not possible to use LW-SSO without setting the **initString** parameter.
- The **initString** parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.
- The **initString** parameter should be shared only between applications integrating with each other using LW-SSO.
- The **initString** parameter should have a minimum length of 12 characters.

- **Enable LW-SSO only if required.** LW-SSO should be disabled unless it is specifically required.
- **Level of authentication security.** The application that uses the weakest authentication framework and issues a LW-SSO token that is trusted by other integrated applications determines the level of authentication security for all the applications.

It is recommended that only applications using strong and secure authentication frameworks issue an LW-SSO token.

- **Symmetric encryption implications.** LW-SSO uses symmetric cryptography for issuing and validating LW-SSO tokens. Therefore, any application using LW-SSO can issue a token to be trusted by all other applications sharing the same **initString** parameter. This potential risk is relevant when an application sharing an initString either resides on, or is accessible from, an untrusted location.

- **User mapping (Synchronization).** The LW-SSO framework does not ensure user mapping between the integrated applications. Therefore, the integrated application must monitor user mapping. We recommend that you share the same user registry (as LDAP/AD) among all integrated applications.

  Failure to map users may cause security breaches and negative application behavior. For example, the same user name may be assigned to different real users in the applications.

  In addition, in cases where a user logs onto an application (AppA) and then accesses a second application (AppB) that uses container or application authentication, the failure to map the user will force the user to manually log on to AppB and enter a user name. If the user enters a different user name than was used to log on to AppA, the following behavior can arise: If the user subsequently accesses a third application (AppC) from AppA or AppB, then they will access it using the user names that were used to log on to AppA or AppB respectively.

- **Identity Manager**. Used for authentication purposes, all unprotected resources in the Identity Manager must be configured with the **nonsecureURLs** setting in the LW-SSO configuration file.

- **LW-SSO Demo mode**.
  - The Demo mode should be used for demonstrative purposes only.
  - The Demo mode should be used in unsecured networks only.
  - The Demo mode must not be used in production. Any combination of the Demo mode with the production mode should not be used.

Troubleshooting and Limitations

This section contains the troubleshooting and limitations for LW-SSO authentication.

➤ "Known Issues" on page 937

➤ "Limitations" on page 938

Known Issues

This section describes known issues for LW-SSO authentication.

➤ **Security context.** The LW-SSO security context supports only one attribute value per attribute name.

Therefore, when the SAML2 token sends more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

Similarly, if the IdM token is configured to send more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

➤ **Multi-domain logout functionality when using Internet Explorer 7**. Multi-domain logout functionality may fail under the following conditions:

The browser used is Internet Explorer 7 and the application is invoking more than three consecutive HTTP 302 redirect verbs in the logout procedure.

In this case, Internet Explorer 7 may mishandle the HTTP 302 redirect response and display an **Internet Explorer cannot display the webpage** error page instead.

As a workaround, it is recommended to reduce, if possible, the number of application redirect commands in the logout sequence.

Limitations

Note the following limitations when working with LW-SSO authentication:

- **Client access to the application**.

  If a domain is defined in the LW-SSO configuration:

  - The application clients must access the application with a Fully Qualified Domain Name (FQDN) in the login URL, for example, http://myserver.**companydomain**.com/WebApp.
  - LW-SSO cannot support URLs with an IP address, for example, http://192.168.12.13/WebApp.
  - LW-SSO cannot support URLs without a domain, for example, http://myserver/WebApp.

  If a domain is not defined in the LW-SSO configuration: The client can access the application without a FQDN in the login URL. In this case a LW-SSO session cookie is created specifically for a single machine without any domain information. Therefore, the cookie is not delegated by the browser to another, and does not pass to other computers located in the same DNS domain. This means that LW-SSO does not work in the same domain.

- **LW-SSO framework integration.** Applications can leverage and use LW-SSO capabilities only if integrated within the LW-SSO framework in advance.
- **Multi-Domain Support**.
  - Multi-domain functionality is based on the HTTP referrer. Therefore, LW-SSO supports links from one application to another and does not support typing a URL into a browser window, except when both applications are in the same domain.
  - The first cross domain link using **HTTP POST** is not supported.

    Multi domain functionality does not support the first **HTTP POST** request to a second application (only the **HTTP GET** request is supported). For example, if your application has an HTTP link to a second application, an **HTTP GET** request is supported, but an **HTTP FORM** request is not supported. All requests after the first can be either **HTTP POST** or **HTTP GET**.

- LW-SSO Token size:

  The size of information that LW-SSO can transfer from one application in one domain to another application in another domain is limited to 15 Groups/Roles/Attributes (note that each item may be an average of 15 characters long).

- Linking from Protected (HTTPS) to non-protected (HTTP) in a multi-domain scenario:

  Multi domain functionality does not work when linking from a protected (HTTPS) to a non-protected (HTTP) page. This is a browser limitation where the referer header is not sent when linking from a protected to a non-protected resource. For an example, see: http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP

- Third-Party cookie behavior in Internet Explorer:

  Microsoft Internet Explorer 6 contains a module that supports the "Platform for Privacy Preferences (P3P) Project," meaning that cookies coming from a Third Party domain are by default blocked in the Internet security zone. Session cookies are also considered Third Party cookies by IE, and therefore are blocked, causing LW-SSO to stop working.

  To solve this issue, add the launched application (or a DNS domain subset as *.mydomain.com) to the Intranet/Trusted zone on your computer (in Microsoft Internet Explorer, select **Menu** > **Tools** > **Internet Options** > **Security** > **Local Intranet** > **Sites** > **Advanced**), which causes the cookies to be accepted.

  Caution: The LW-SSO session cookie is only one of the cookies used by the Third Party application that is blocked.

- **SAML2 token.**

  - Logout functionality is not supported when the SAML2 token is used.

    Therefore, if the SAML2 token is used to access a second application, a user who logs out of the first application is not logged out of the second application.

- The SAML2 token's expiration is not reflected in the application's session management.

  Therefore, if the SAML2 token is used to access a second application, each application's session management is handled independently.

- **JAAS Realm.** The JAAS Realm in Tomcat is not supported.
- **Using spaces in Tomcat directories.** Using spaces in Tomcat directories is not supported.

  It is not possible to use LW-SSO when a Tomcat installation path (folders) includes spaces (for example, Program Files) and the LW-SSO configuration file is located in the **common\classes** Tomcat folder.

- **Load balancer configuration.** A load balancer deployed with LW-SSO must be configured to use sticky sessions.
- **Demo mode**. In Demo mode, LW-SSO supports links from one application to another but does not support typing a URL into a browser window, due to an HTTP referrer header absence in this case.

Part VIII

User-Defined Templates

38

SiteScope Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

SiteScope Templates Overview

Templates provide an enterprise solution for standardizing the monitoring of the different IT elements in your enterprise, including servers, applications, databases, network environments, and so forth. You use templates to rapidly deploy sets of monitors that check systems in the infrastructure that share similar characteristics.

SiteScope provides the following types of templates:

- User-defined templates (discussed in this chapter).
- Predefined solution templates. For details, see "SiteScope Solution Templates" on page 1083.
- Monitor Deployment Wizard templates. For details, see "Monitor Deployment Wizard Templates and Variables" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

Advantages of Using SiteScope Templates

- You can create and customize your own templates to meet the requirements of your organization.
- SiteScope templates are used to standardize a set of monitor types and configurations into a single structure. This structure can then be repeatedly deployed as a group of monitors targeting multiple elements of the monitored environments.
- Templates speed the deployment of monitors across the enterprise through the single-operation deployment of groups, monitors, alerts, remote servers, and configuration settings.

- Templates provide the ability to view how the actual monitored deployments comply with the standardized deployment as defined in the template. This ensures that any changes in the monitored environment can be quickly updated in the monitoring infrastructure and that the monitoring infrastructure is still compliant with the standards set in the template.
- You can deploy multiple templates simultaneously instead of deploying each template separately. You can also perform mass deployments of the same template using a CSV file external to the SiteScope user interface. For the various ways of deploying templates, see "Deploy SiteScope Templates Overview" on page 1012. For details about deploying templates using a CSV file, see "Deploying a Template Using a CSV File" on page 1013.
- You can use silent template deployment to submit deployment requests, and continue to use SiteScope without having to wait for the template deployment process to finish. The template deployment requests are queued and processed in the background. If SiteScope restarts before all requests in the queue are complete, it automatically continues the deployment process after the restart.
- You can make changes to the template, and publish the changes to all SiteScope objects deployed by the template using the Publish Template Changes Wizard. If a change is required to a template object, for example, a threshold value changes or a new monitor or alert is required, you can update the template once and publish the changes to all deployed groups without having to update each object individually. For details about publishing changes, see "Publish User-Defined Templates" on page 1031.
- Export and import templates for use in other SiteScope installations. This enables you to replicate standardized monitor configurations across the enterprise. For details about exporting and importing templates, see "Import or Export Templates" on page 1003.

Understanding Templates

Templates are objects you use to reproduce groups, servers, monitors, and alerts according to a predefined pattern and configuration. You can deploy all of the items defined in the template in a single operation by copying the template to a location in the SiteScope hierarchy. Templates also use template variables that you use to interactively set certain monitor, server, and alert configuration settings when you deploy the template. Once you have created a template, you can use it to deploy monitors as often as needed.

The following methods are used for adding configurations to the created template.

- Copy an existing group and monitor hierarchy from a SiteScope to the template and edit the elements for use as a template. For details, see "How to Create a Template by Copying Existing Configurations" on page 973.
- If there are no applicable SiteScope monitor elements in your enterprise or if you want to create new objects or settings, you can manually create template groups, monitors, servers, and alerts in the template. For details, see "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964.

Tips:

- If SiteScope monitoring has not yet been configured and you are not familiar working with SiteScope monitors and groups, you should set up some sample groups, monitors, and alerts before you create templates. This helps familiarize you with the monitor configurations and the relationship between monitors, groups, and alerts. Afterwards, you can copy the structure from the SiteScope and convert the configurations to a template.
- To help you get started with templates, SiteScope provides example templates for monitoring in Windows and UNIX environments. For details, see "Template Examples" on page 950.

This section includes:

Template Elements and Features

You create templates within a template container in the template view. These elements are then displayed in the template tree where you can access them for changes or deployment. For more information, see "Understanding Templates" on page 946.

You use templates to deploy a standardized pattern of monitoring to multiple elements in your infrastructure. Effective development and use of templates requires some planning because you can add multiple objects types to the template. For more information, see "Planning Templates" on page 951.

You create a template by adding and configuring groups, remote server definitions, monitors, alerts, and variables to the template. You use template variables as substitution markers for configuration settings that you want to change dynamically or interactively each time you deploy the template. Creating and referencing variables is an action that is unique to templates. For more information, see "Working with Template Variables" on page 953.

Several SiteScope monitor types use a measurement counter browser function to dynamically query applications and systems for the metrics that are available for monitoring. When you create one of these monitors manually, you use a multiple step procedure to view and select counters. An alternative method is used to select counters when deploying templates. For details, see "How to Modify Counter Selection Strings to Use Regular Expressions" on page 975.

After you create and configure templates, you deploy them in the SiteScope hierarchy. For details on deploying templates, see "Deploy the template" on page 971. If you subsequently want to make changes to the source template, you can automatically publish the changes to SiteScope objects deployed by the template using the Publish Template Changes Wizard. For details on updating templates, see "Updating Template Deployments" on page 1032.

If you want to use templates in other SiteScope installations, you can save the template to a file, and copy the export file to another SiteScope server and import the template container object that contains the templates you want to use. For details on exporting and importing templates, see "Import or Export Templates" on page 1003.

Note:

- For information on configuring internal properties in SiteScope templates, refer to the HP Software Self-solve knowledge base (h20230.www2.hp.com/selfsolve/documents). To enter the knowledge base, you must log on with your HP Passport ID.
- You can also use the SiteScope API when working with templates. For details, see "Using the SiteScope Configuration API" on page 42.

Template Objects

Templates are created and stored in a template container in the template tree. The template variable definitions and SiteScope objects configurable using the template are displayed as objects within the template.

The following table describes the objects used in templates:

Icon	Object Type	Description
	Template Container	A template container enables you to manage your template monitoring solutions. You can add a template to a template container only. For details on configuring this object, see "New Template Container Dialog Box" on page 982.
	Template	The template contains the SiteScope group, monitors, remote servers, variable definitions, and alerts that make up the template monitoring solution. For details on configuring this object, see "New Template Dialog Box" on page 983.

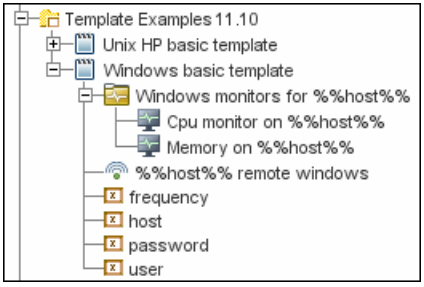
Icon	Object Type	Description
	Template Variable	A variable is used to prompt for user input during template deployment. Template variables are either user-defined or predefined system variables. For details on configuring this object, see "New Variable Dialog Box" on page 986.
	Template Remote Server	A template remote server is used to define Windows or UNIX remote server preferences that are created when the template is deployed. For details on configuring this object, see "New Template Remote Server Dialog Box" on page 989.
	Template Group	A template group contains the template monitors and associated alerts. You use template groups to manage the deployment of monitors and associated alerts in your infrastructure. For details on configuring this object, see "New Template Group Dialog Box" on page 991.
	Template Monitor	Template monitors are used to define monitors that are created when the template is deployed. For details on configuring this object, see "New Template Monitor Dialog Box" on page 997.
	Template Alert	Template alerts are used to define alerts on groups and monitors that are created when the template is deployed. If an alert has been set up for the template monitor or group, the alert symbol is displayed next to the monitor or group icon. For details on configuring this object, see "New Alert Dialog Box" on page 1000.

Template Examples

SiteScope provides template examples for monitoring in Windows and UNIX environments. These templates are available from the **Template Examples 11.10** folder in the template tree. You can use the template examples to help familiarize you with using SiteScope templates. Among other things, you can use it to see the following:

- How template groups, monitors, and remote servers are used
- The connection between the template remote server and the monitor using it
- Variable value usage and system variable usage

The following example shows the **Windows basic template**. The template contains a template group, **Windows monitors for %%host%%**, two template monitors (CPU and Memory), four user-defined variables (host, user, password, and frequency), and a template remote server.



Planning Templates

Template planning is important for effective SiteScope management. You should consider the group and monitor relationships and properties in the template structure and how it fits into the overall monitoring environment.

The following are things to consider as you plan templates:

Object	Consideration
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 953.
Servers	Decide which servers are the target servers. This is where the objects being monitored are located. Template servers are replicated automatically when the template is deployed. You can also define them manually in the Microsoft Windows Remote Servers or UNIX Remote Servers container of the remote server tree. For more information, see "Remote Servers Overview" on page 584.
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.

Object	Consideration
Common properties	For configuration properties that should be the same from one template deployment to another, you must decide what the values should be. For example, the **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 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 affect 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 (see "SiteScope Alerts Page" on page 1461). For example, a template alert added to a template group alerts on any monitor belonging to that group. If this does not fit your alerting plan, you must edit the alert configuration after deployment or add alerts manually.

Working with Template Variables

While you can create templates without using template variables, the use of variables is central to the power and utility of templates. Template variables are substitution markers for monitor configuration settings. You create template variables to represent monitor configuration settings that you want to be able to modify whenever you deploy the template. You reference the variable in a text box in one or more template monitors. Each variable that is referenced in a monitor or group object in a template prompts the display of a corresponding entry box when the template is deployed. The variable name is used as a label for the text entry box.

Examples of common uses for template variables are:

- Server or host addresses
- Disk drive designators
- File paths
- Monitor name descriptions

Note: You can see examples of variables used in templates in the **Template Examples 11.10** folder in the template tree. For details, see "Template Examples" on page 950.

Guidelines for Using Template Variables

- You should plan and create the template variables before you create other template objects, such as servers and monitors. This enables you to enter the references to the variables into the template monitors, groups, or alerts as you add them to the template. Deleting a template variable that has already been referenced in a template object requires that the referencing object be deleted from the template to clear the broken reference. For details on referencing template variables, see "Referencing Template Variables" on page 957.
- Some monitor configuration settings cannot be set using template variables. With the exception of the remote server selection menu, configuration items that are normally selected using a selection drop-down cannot be defined using template variables. Configuration items that are normally selected using a check box or radio selection cannot be configured using template variables.
- Template variables are always child elements of the template container in which they reside. Variables can be referenced and used to define configuration settings for group, monitor, or alert configuration templates within the template. For information about the types of template variables in SiteScope and the specific syntax conventions, see "Variable Syntax" on page 955.

This section contains the following topics:

Variable Syntax

The following types of template variables are available in SiteScope:

- **User-defined variables.** They are used to enter text-based values during template deployment. User-defined variables must have the "%%" symbol either side of the variable name.
- **System variables.** A set of predefined variables you use to access both the list of remote servers known to SiteScope and system time information. System variables must have the "$$" symbol either side of the variable name.

Note: User-defined and pre-defined system variables are available in all the text fields and text table cells when configuring templates.

Each type of variable has specific syntax conventions which are described in the following sections.

Syntax for User-Defined Variables

User-defined template variables can contain only alphanumeric characters and the underscore character. You can create as many variables as you need.

Examples of valid template variable syntax are:

```
description_text
DiskDrive
TARGET_URL
matchExpression
```

You should choose variable names that describe the configuration parameter that is represented. The variable name is used as a label for the variable entry box on the variable value entry window when you deploy the template.

Syntax for System Variables

SiteScope recognizes several pre-defined template variables. These are values that are known by the system, including the list of servers for SiteScope, detected servers such as NetBIOS, and user-defined server connection profiles such as remote UNIX. The syntax and description for the pre-defined system variables are:

Syntax for System Variables	Description
$$SERVER_LIST$$	Returns a list from which to select one of all the servers known by the platform. Use this to enable selection of remote servers for **Server** or **Host Name** properties only.
$$SERVER_NAME$$	Derived from the $$SERVER_LIST$$ variable. Returns the name of the current server with \\ (backslashes) before the name. Use when referencing the server in other boxes.
$$SERVER_NAME_BARE$$	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 box requiring just the name of the server (for example, when deploying CPU monitors or when referencing the name of the server in a description: "Disk space on server Mail.")
$$DATE$$	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 represents the time that the template is deployed.

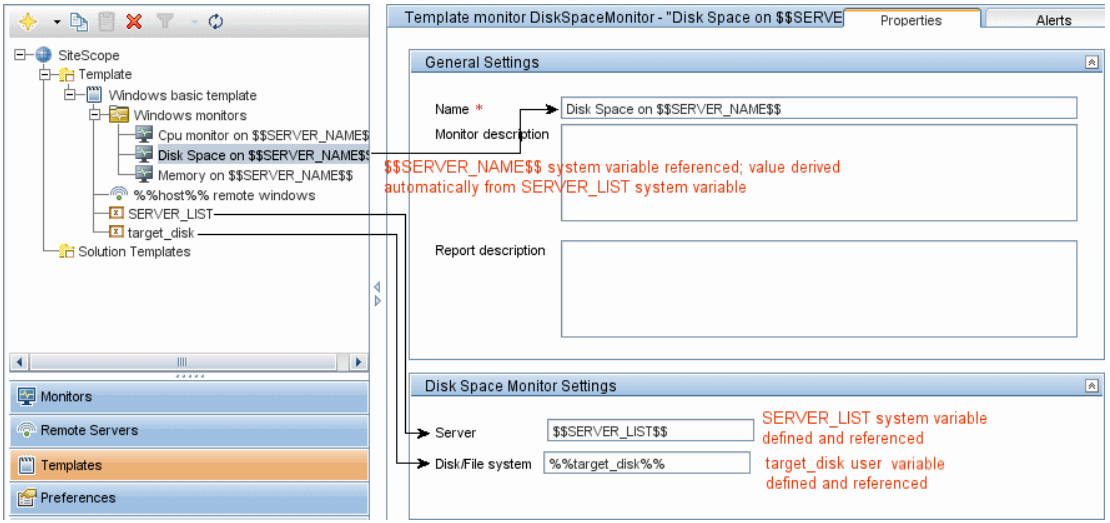
Referencing Template Variables

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.

Variable Type	Syntax	Information
User-Defined	%%variable_name%%	The reference is case sensitive and syntax sensitive. **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.
System	$$VARIABLE_NAME$$	The reference is case sensitive and syntax sensitive. The $$SERVER_LIST$$ variable must be defined explicitly as a variable in the template. After this variable is defined, the $$SERVER_NAME$$ and $$SERVER_NAME_BARE$$ variables may be used in configuration objects by referencing them using the $$VARIABLE_NAME$$ syntax directly in the monitor or group configuration object. The $$TIME$$ and $$DATE$$ variables can also be referenced directly. For information about system variables, see "Variable Syntax" on page 955.

Example - Referencing User-Defined and System Variables

The following shows examples of how to reference user-defined variables and the $$SERVER_LIST$$, and the derived system variables for a monitor template.



Counter Selection in Monitor Templates

SiteScope includes a number of application monitor types that are designed to monitor measurements specific to the target system. These browsable counter monitor types use a **Get Counters/Measurements** browser function in the Monitor Settings pane. Configuring these monitor types manually requires the following steps after selecting the monitor type:

- Specifying connection properties to the target system and then requesting that SiteScope retrieve the measurement counters from the remote system.
- Selecting the desired counters to be monitored and adding them to the configuration. After this, the monitor can be added to SiteScope.

Deploying monitors using templates does not accommodate a separate step for counter selection. Another mechanism is used to enable the selection of counters for these monitor types using templates. SiteScope uses text matching or regular expression matching to automate the counter selection step for template deployment. You use a counter selection step when you create the template monitor.

The simplest method for counter selection in templates is to select the specific counters explicitly in the monitor template. This creates an explicit text match used to select the matching counter during deployment. For information about the steps required to add a browsable counter monitor type with explicitly selected counters, see "Create template monitor instances" on page 968.

If the specific counters on the target system vary from one deployment to another, you may be able to use a regular expression to match a pattern that represents the type or category of counter you want to monitor. For more information, see below.

This section contains the following topics:

Modifying Counter Selection Strings to Use Regular Expressions

You can modify counter selection strings for template monitors to use regular expressions when you create the monitor, or you can edit the monitor later. For more information on modifying a template monitor for regular expression counter matching, see "How to Modify Counter Selection Strings to Use Regular Expressions" on page 975.

Counter Selection Using Regular Expressions

Many applications have a number of measurement counters that vary according to the system on which it is running, the configuration of system options, and the components installed. In this case, selecting explicit counters in a monitor template may not be useful across multiple instances of an application or system. Some systems have measurement counters that have a similar pattern but may vary by the name of a node or object context. You can use regular expressions in monitor templates to help automate the selection of multiple measurement counters.

Note: Use of this regular expression counter matching function requires knowledge of the counters on the system to be monitored. You should manually set up a monitor of the type you want to add to the template and carefully review the counters available on the type of system you want to monitor. Creating a "greedy" regular expression that matches large numbers of counters on a remote system may adversely affect SiteScope performance.

The steps you use to create a template monitor to use regular expressions are very similar to the procedure described in the previous section. Instead of selecting all of the counters to be monitored explicitly, you select one or more counters that are representative of all the counters you want to select. The counter selections in monitor templates are stored as text strings. You edit these strings to create patterns that SiteScope uses to find matching counters that are selected when the monitor is deployed.

Note: When using regular expressions to select measurement counters or match thresholds, SiteScope checks only whether one string is a substring of another, rather than performing an equality check. This means that the incorrect set of counters and thresholds could be defined in the monitor after deployment. For example, if the chosen monitor threshold is x/y, and x/yy also matches the regular expression, this threshold is also defined.

Example - Using Regular Expressions

➤ **Example 1.** The following is a simple example of how a regular expression can be used for counter selection for a SNMP by MIB Monitor type in a template:

You want to monitor the following three counters from several SNMP agents in your infrastructure:

```
iso/org/dod/internet/mgmt/mib-2/system/sysDescr
iso/org/dod/internet/mgmt/mib-2/system/sysUpTime
iso/org/dod/internet/mgmt/mib-2/system/sysName
```

You could select all three counters explicitly in the template monitor. Alternately, you could select one of these and then modify the counter string to be a regular expression such as the following:

```
/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. Because the selection string included several / slash characters initially, each of these characters must be escaped by adding a \ backslash character immediately preceding it. The [DUN][a-zT]* string includes two character class declarations commonly used in regular expression syntax. For more information on regular expression syntax, see "Using Regular Expressions" on page 235.

➤ **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. Because these characters have special meaning in regular expressions, they would have to be escaped. This can be complicated because the process strings have many variations and combinations of these and other symbols.

The example regular expression used here simplifies the expression by using character class declarations. The [\W] class is used to match punctuation marks. This matches on the \, -, :, and / characters that appear in some of the process strings without the need to escape the characters individually. For more information on regular expression syntax, see "Using Regular Expressions" on page 235.

Maximum Number of Counters That Can be Saved

Browsable monitors are limited by the number of counters they have. The maximum number of counters is determined by the **_browsableContentMaxCounters** parameter in the **master.config** file (also in **Preferences > Infrastructure Preferences > Monitor Settings > Maximum browsable counters to be selected**). If you create or edit a monitor so that it has more counters than this value, only the number of counters up to this value is saved.

When a browsable monitor is deployed in a template, the number of counters that match the selected patterns are limited by the **_maxCountersForRegexMatch** parameter in the **master.config** file. If, during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved.

The **_maxCountersForRegexMatch** parameter is also used to limit the number of counters that match the selected counter patterns when creating and updating dynamic monitors. We recommend using the same value for both **_browsableContentMaxCounters** and **_maxCountersForRegexMatch** parameters in the **master.config** file. The default value for both of these parameters is 1000.

When upgrading from earlier versions of SiteScope, the value for both of these parameters is set to the higher of these two parameter values in the previous version, or to 1000 (whichever is greater).

Tasks

How to Configure a SiteScope Monitoring Solution Using a Template

This task describes the steps for creating a SiteScope monitoring solution using a user-defined template. To view a flowchart of this task, see "How to Configure a SiteScope Monitoring Solution Using a Template – Flowchart" on page 62. For details on using predefined solution templates, see "SiteScope Solution Templates" on page 1083.

Tips:

- We recommend that you create template objects in the order listed. You can skip the steps for any template objects that you do not require.
- To help you get started with templates, SiteScope provides example templates for monitoring in Windows and UNIX environments. For details, see "Template Examples" on page 950.

Note: Some fields that contain drop-down lists when configuring objects in normal mode, are displayed as text boxes when configuring the object in template mode.

This task includes the following steps:

- "Prerequisites" on page 965
- "Create a template container" on page 965
- "Create a template" on page 965
- "Create template variables" on page 966

1 Prerequisites

➤ Check that the post-installation administration tasks have been performed before configuring SiteScope for monitoring. For task details, see "How to Setup and Administer SiteScope" on page 55.

➤ To deploy a template, regardless of its content, you must have edit permissions on the deployment target group. You do not need edit permissions on the template objects (monitors, remotes, and alerts). For details on user permissions, see "New/Edit User Profile Dialog Box" on page 870.

2 Create a template container

Create a template container to enable you to manage your monitoring solution.

For user interface details, see "New Template Container Dialog Box" on page 982.

3 Create a template

Add a template to the template container. This is the container for your monitoring solution, in which you create groups, monitors, remote server, variables, and alerts for the monitoring solution. You can create multiple templates in a template container.

For user interface details, see "New Template Dialog Box" on page 983.

Note: You can also copy an existing group and monitor hierarchy from a SiteScope to the template and edit the elements for use as a template. For task details, see "How to Create a Template by Copying Existing Configurations" on page 973.

---

4 Create template variables

You can create template variables in the template that enable you to specify a different name for an object every time that you deploy the template. Variables should be the first objects you create in a template, because they are referred to when you create groups, monitors, servers, and alerts.

a Create the template variable in the template. For more information on the user interface, see "New Variable Dialog Box" on page 986.

b Reference the variable in one or more configuration objects in the template. For more information on this topic, see "Referencing Template Variables" on page 957.

Note:

- If a remote server is specified with a variable name with no additional characters prefixed or suffixed to it (for example, %%hostname%%), and the same variable is specified for any field in a monitor, after deployment the value appears as **Remote-##** on UNIX and \\<**variable_value**> on Windows, instead of just the variable value that was specified on deployment. To avoid this, where a variable name is used for a remote server, additional characters should be prefixed or suffixed to the name.
- User-defined and pre-defined system variables are available in all the text fields and text table cells when configuring templates.

---

5 Create a template remote server

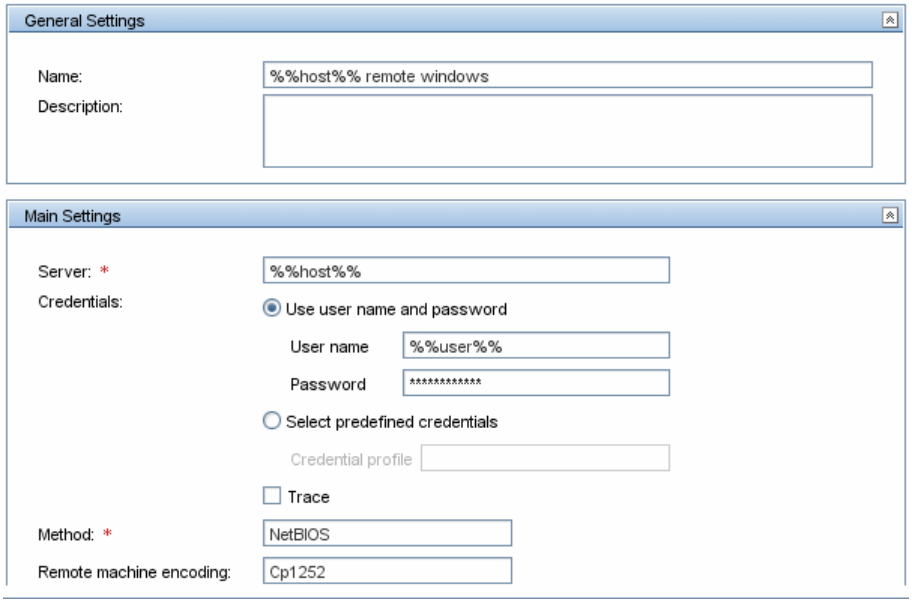
In the template, you can define a remote Windows or UNIX server where the monitored objects are located. A template monitor may run on servers that are defined by template servers at the time of template deployment or on servers defined manually in Remote Servers. Template servers are added to the remote server tree under Microsoft Windows Remote Servers or UNIX Remote Servers when the template is deployed.

For user interface details, see "New Template Remote Server Dialog Box" on page 989.

Note: You can add only one remote server to a template. This does not apply to templates created in versions of SiteScope earlier than 9.50.

Example:

A Windows template remote server has been created with the name %%host%% remote windows.



6 Create a template group

In the template, create a template group to make the deployment of monitors and associated alerts manageable and effective for your organization.

For user interface details, see "New Template Group Dialog Box" on page 991.

Note:

- By default, monitors must be created in a template group. You can override this setting in **Preferences** > **Infrastructure Preferences** > **Template Settings** by selecting **Allow creation of template monitors directly under template entity**.
- You can also define a template group so that its content is not a part of the template, and is ignored, when publishing changes to deployed groups. This enables deploying templates inside different deployed groups. For details, see "Ignore group when publishing changes" on page 993.
- A template can have only one template group directly under it (the parent group). This does not apply to templates created in versions of SiteScope earlier than 9.50.

---

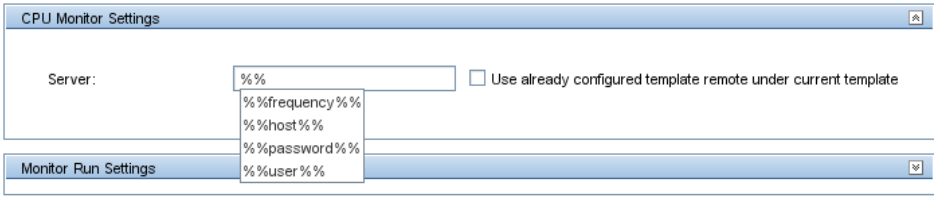
7 Create template monitor instances

a Select the monitor instances you want to add to the template group. For user interface details, see "New Template Monitor Dialog Box" on page 997.

b Enter values for the monitor properties.

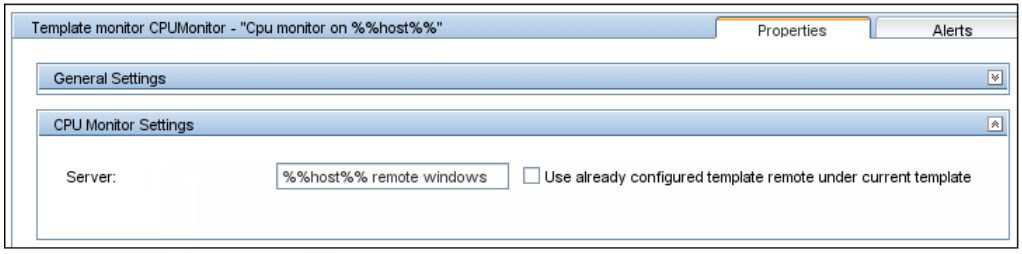
- If you are using template variables, enter the variable syntax for all fields whose values are to be replaced with a variable. This includes use of the $$SERVER_LIST$$ system variable. For concept details, see "Syntax for System Variables" on page 956.

➤ To enter a variable, type either %% or $$. The list of available variables of that type is displayed automatically. Click the relevant variable to select it (using the keyboard to navigate through the list of available variables is not supported). The variable is then displayed in the field.



Example of using a variable when configuring a monitor:

In this example, the template monitor (a SiteScope CPU monitor) is configured to run on the template remote server, %%host%% remote windows.



Note:

- A template monitor can run on servers that are defined by template servers at the time of template deployment or on servers defined manually in the Remote Servers container of the remote server tree. Whichever is the case, the value in the **Server** box must match the host name of an actual server at the time that the template is deployed after values have been substituted for the template variables. If the server name does not match the host name of a real server, the monitor fails. To automatically retrieve the template remote server name (if one was created), select the **Use already configured template remote under current template** check box in the Monitor Settings field. For user interface details, see "New Template Monitor Dialog Box" on page 997.
- Do not use "\\" in the monitor **Server** field, and in the remote server **Name** and **Server** fields.
- You can add monitor instances directly to the template entity if you select **Allow creation of template monitors directly under template entity** in **Preferences** > **Infrastructure Preferences** > **Template Settings**.

---

c For monitors with browsable counters, select counters to monitor measurements specific to the target system.

- Click the **Get Counters** button, and select a server or enter the connection information for a server that is running the service or application that you want to monitor.
- Click the **Get Counters** button again to retrieve the available counters. The counter selection dialog box is updated.
- Select the measurements or counters that you want to monitor. If the specific counters on the target system vary from one deployment to another, you can use a regular expression to match a pattern that represents the type or category of counter you want to monitor. For task details, see "How to Modify Counter Selection Strings to Use Regular Expressions" on page 975.

d Configure other monitor settings in the Properties tab, such as:

- Manually set thresholds for monitors by setting logic conditions that determine the reported status of each monitor instance. For user interface details, see "Threshold Settings" on page 457.

Note: After deploying a template, you can also set thresholds for one or multiple monitors using a baseline. For task details, see "How to Set Monitor Thresholds Using a Baseline" on page 418.

- Build dependencies between groups and key monitors to help control redundant alerting. For concept details, see "Monitoring Group Dependencies" on page 397.
- For the complete list of common user settings, see "Common Monitor Settings" on page 447.

8 Set up monitor and group alerts

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

For task details, see "How to Configure an Alert" on page 1443.

9 Deploy the template

After creating a SiteScope monitoring template, you can deploy templates to a group.

- You can deploy a single template, or multiple templates simultaneously to a group from the user interface. For task details, see "How to Deploy Templates Using the User Interface" on page 1014.
- You can perform mass deployments of a single template using a CSV file external to the SiteScope user interface. A CSV file is better suited for performing mass deployments, since it is easier to enter and update all the template variable values in one CSV file. For concept details, see "Deploying a Template Using a CSV File" on page 1013. For task details, see "How to Deploy Template Using a CSV File" on page 1017.

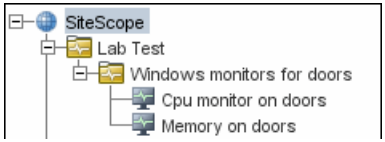
➤ You can deploy a template using an XML file external to the SiteScope user interface. For concept details, see "Auto Template Deployment Overview" on page 1054. For task details, see "How to Deploy a Monitoring Structure Using an XML File" on page 1064.

10 Results

SiteScope adds the groups, monitors, and alerts to the specified group in the monitor tree.

Example:

The template example, **Windows basic template**, was deployed to a group container named **Lab Test**. It contains a **CPU monitor** and **Memory monitor**, and was deployed to monitor resource usage on a server named **doors**.



11 Set up monitor and group reports (in the monitor view)

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

For task details, see "How to Create a Report" on page 1508.

12 Publish changes to the monitoring solution

You can make changes to deployed templates, for example, by adding or removing monitors or modifying monitor properties. You do this by editing the template and using the Publish Template Changes Wizard to publish the changes to all the relevant objects deployed by the template.

For task details, see "How to Publish Template Updates to Related Group Deployments" on page 1035.

How to Create a Template by Copying Existing Configurations

This task describes the steps involved in copying an existing group, monitor, or remote server from a SiteScope to the template and editing the elements for use as a template.

This task includes the following steps:

1 Prerequisites

Before copying an existing configuration from a SiteScope to a template, the template container and template into which you want to copy the entity must exist in the template tree.

Note: When copying an existing monitor or remote server to a template, a template group must also exist in the template.

For details on creating a template container, template, and template group, see "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964.

2 Copy the configuration to the template

Right-click the group, monitor, or remote server you want to copy, and select **Copy to Template**. In the Copy to template tree dialog box, select the template or template group to which you want to add the copied configurations.

For user interface details, see "Copy to Template Tree Dialog Box" on page 489.

3 Edit template variables

If you are using template variables in the new template, edit each copied object by replacing the applicable configuration field's value with the required variable syntax.

For concept details, see "Referencing Template Variables" on page 957.

4 Results

SiteScope adds the group, monitor, or remote server to the specified template or template group in the template tree.

How to Modify Counter Selection Strings to Use Regular Expressions

This task describes the steps involved in modifying a template monitor to use a regular expression for measurement counter selection.

Note: This task applies to monitors with browsable counters only.

---

1. In the template tree, click the monitor template you want to modify to open the template monitor Properties view.
2. Open the Monitor Settings pane, and in the **Measurements** or **Counters** section (depending on the monitor type), select a counter selection string that is representative of the pattern of counters you want to configure for the monitor.
3. Modify the counter selection string to be a regular expression by adding a slash ("/")character to the beginning and end of the string. Modify the string to use other pattern matching syntax as required. For more information on regular expression syntax, see "Using Regular Expressions" on page 235.

Note: If the template monitor was configured with explicit counter selections that can be matched using the regular expression that was entered, you can delete the extra counter strings by clicking the **Delete Counter** button.

Reference

Reserved Template Group Types

The following table shows template types used by the SiteScope application. The templates in these directories are reserved, and are not used by alerts. For a list of templates used in alerts, see "SiteScope Alert Templates Directory" on page 1450.

Note: We do not recommend modifying the templates in these directories without following the specific procedures provided in the product documentation or as instructed by HP Software Support.

Template Group	Description	Location
MIB	Text used with SNMP traps	<SiteScope root directory>\templates.mib
Operating System	Shell commands to be run when monitoring remote UNIX servers	<SiteScope root directory>\templates.os
Performance Monitor	Used for NT performance monitoring	<SiteScope root directory>\templates.perfmon
Sound	Audio files used for sound alerts	<SiteScope root directory>\templates.sound
View	Query and XML/XSL templates	<SiteScope root directory>\templates.view

SiteScope Templates User Interface

This section includes:

SiteScope Templates Page

This page displays the name and description of the selected template container. Use this page to add template containers, or edit the properties of existing template containers (not Solution Templates).

To access	Open the **Templates** context. In the template tree, select the **SiteScope** node.
Important information	You can also use the SiteScope API when working with templates. For details, see "Using the SiteScope Configuration API" on page 42.
Relevant tasks	"How to Configure a SiteScope Monitoring Solution Using a Template" on page 964
See also	"Template Tree" on page 95

User interface elements are described below:

UI Element	Description
	**New Template Container.** Opens the New Template Container dialog box, enabling you to create a new template container. For user interface details, see "New Template Container Dialog Box" on page 982.
	**Edit Template Container.** Enable editing the selected template container.
	**Delete Template.** Deletes the template container.
<SiteScope Templates table>	Lists the predefined template that come with SiteScope (Template Examples, Monitor Deployment Wizard Templates, and Solution Templates), and any user-defined template containers. Double-click a template container to open the template container page for the selected template.
Name	Name string assigned to the template container.
Description	Description of the template container that was assigned when creating or editing the template container.

Templates Tree - Properties Page

This page displays the name and description of the selected template object. In the template tree, select a template object (template group, template monitor, template variable) to display properties for the specific object. Use this page to edit the properties of the template.

To access	Select the **Templates** context. In the template tree, select a template object to display properties for the object. The template Properties tab is displayed only when a template group or monitor is selected.

Relevant tasks	"How to Configure a SiteScope Monitoring Solution Using a Template" on page 964
See also	"Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
Name	The template name.
Description	Description of the template.
Last edited by	SiteScope user that last edited the template. This field is read-only. **Note:** This field is displayed only when a template is selected in the template tree.
Last edited on	Time and date that the template, or any object within the template, was last edited. This field is read-only. **Note:** This field is displayed only when a template is selected in the template tree.

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Existing Tag	Click to add existing tags. The Search/Filters dialog box opens. For details, see "Search/Filters Tag Dialog Box" on page 1001.

Templates Tree - Alerts Tab

This tab displays a list of alerts associated with the solution template. Use this page to add, delete, or edit alerts associated with the template. In the template tree, select a template group or monitor to display alerts for the selected object.

To access	Select the **Templates** context. In the template tree, navigate to the group or monitor to which you want to view, add, or edit alerts. Click the **Alerts** tab.
Relevant tasks	➤ "How to Deploy a SiteScope Solution Template" on page 1088 ➤ "How to Configure an Alert" on page 1443
See also	➤ "Template Tree" on page 95 ➤ "SiteScope Alerts Page" on page 1461

User interface elements are described below:

UI Element	Description
	**New Alert.** Opens the New Alert dialog box enabling you to define a new alert. For user interface details, see "New/Edit Alert Dialog Box" on page 1463.
	**Edit Alert.** Opens the Edit Alert dialog box enabling you to edit the alert. For user interface details, "New/Edit Alert Dialog Box" on page 1463.
	**Copy Alert.** Copies the alert.
	**Paste Alert.** Pastes the alert.
	**Delete Alert.** Deletes the alert.
Name	Name string assigned to the alert definition.
Status	The enabled/disabled status of the alert. ➤ **Enabled.** Overrides any disable action on the alert and enables the alert for execution based on the conditions defined. ➤ **Disabled 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. ➤ **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.
Description	Description of the alert definition that was assigned when creating or editing the alert.
Action Name	Name given to the action to be done when the alert is triggered. It is not the name of the alert.

New Template Container Dialog Box

This dialog box enables you to define a new template container. You use template containers to store and manage templates. Template containers enable you to group and organize multiple templates in ways that describe their purpose or classification.

To access	Select the **Templates** context. In the template tree, right-click the SiteScope node or an existing template container, and select **New** > **Template Container**.
Important information	➤ Template containers can be added only to the SiteScope node in the template tree. ➤ Templates are displayed with the  icon in the template tree. Template containers can hold templates only.
Relevant tasks	➤ "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964 ➤ "How to Create a Template by Copying Existing Configurations" on page 973
See also	➤ "Understanding Templates" on page 946 ➤ "Template Examples" on page 950 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
Name	Name for the template container. **Maximum length:** 250 characters
Description	Description for the template container.

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

New Template Dialog Box

This dialog box enables you to add a template to a template container. An individual template is comprised of the object definitions of those objects that are created when the template is deployed. Templates are displayed with the icon in the template tree.

To access	Select the **Templates** context. In the template tree, right-click a template container, and select **New** > **Template**.
Important information	➤ A template can have one template group only directly under it (the parent group). This does not apply to templates created in versions of SiteScope earlier than 9.50. ➤ Templates can contain a group and subgroups, variables, and a remote server. They can also contain monitors, provided **Allow creation of template monitors directly under template entity** is selected in **Preferences** > **Infrastructure Preferences** > **Template Settings**.

Relevant tasks	➤ "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964 ➤ "How to Create a Template by Copying Existing Configurations" on page 973
See also	➤ "Understanding Templates" on page 946 ➤ "Template Examples" on page 950 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
Name	Name for the template. The name you enter appears in the template tree as a child node of the template container. **Maximum length:** 250 characters.
Description	Description for the template.
Last edited by	SiteScope user that last edited the template. This field is updated only after the template is created. **Default value:** N/A
Last edited on	Time and date that the template (or any object within the template) was last edited. This field is updated only after the template is created. **Default value:** N/A

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

New Variable Dialog Box

This dialog box enables you to add a template variable to a template. A variable is used to enable prompting for user input during template deployment. Template variables are either user-defined or predefined system variables that provide access to the list of remote server connections known to SiteScope. Template variables are displayed with the icon in the template tree.

To access	➤ Select the **Templates** context. In the template tree, right-click a template, and select **New** > **Variable**. ➤ In the Template <monitor> page, click **New Variable**. For details, see "New Template Monitor Dialog Box" on page 997. ➤ In the New Template Alert dialog box, click **New Variable**. For details, see "New Alert Dialog Box" on page 1000. ➤ In the Alert Action dialog box, click **New Variable**. For details, see "Alert Action Dialog Box" on page 1476. ➤ In the New Microsoft Windows Remote Server dialog box, click **New Variable**. For details, see "New Template Remote Server Dialog Box" on page 989. ➤ In the New UNIX Remote Server dialog box, click **New Variable**. For details, see "New Template Remote Server Dialog Box" on page 989.
Important information	When configuring variables for **Frequency** and **Error frequency** in the Monitor Run Settings, the variable values can only be in time units of seconds.
Relevant tasks	"How to Configure a SiteScope Monitoring Solution Using a Template" on page 964
See also	➤ "Understanding Templates" on page 946 ➤ "Working with Template Variables" on page 953 ➤ "Template Examples" on page 950 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
Name	Name for the template variable. The name you enter is used to identify the variable in the template in the template tree. This is the name that must be used when referring to the variable in other template objects. **Note:** The name of a variable cannot be edited after the variable has been added. To change a variable name, delete the variable and create a new one with the correct name.
Display name	Display name if you want a different name to be displayed instead of the variable name on deployment. You must still use the variable name when referencing the variable in a template object.
Description	Description for the variable.
Default value	Default value to be used for this variable. If you do not enter a value in this box and the box requires a value, you are prompted to enter a value when deploying the template.
Display order in template	Variable display sequence number. This is the order in which SiteScope prompts you to enter values for a variable on deployment. Variables are displayed in ascending order. Variables that have no display number are displayed at the end. **Note:** The display order does not change the order of the variables within the template definition.

UI Element	Description
Password variable	Hides the default value and the value entered during deployment. **Default value:** Not selected **Note:** This option is automatically selected for any variable from previous versions of SiteScope that has a name ending with PASSWORD or password.
Mandatory variable	The variable field requires a value and prompts you to enter a value when deploying the template. To set a variable with a non-mandatory value, clear the check box. When this option is cleared, SiteScope uses an empty String ("") as a value for a non-mandatory variable. **Default value:** Selected

New Template Remote Server Dialog Box

This dialog box enables you to create a UNIX or Windows remote server in the template. A template remote server is used to define remote server preferences that are created when the template is deployed. A template remote server is displayed with the icon in the template tree.

To access	Select the **Templates** context. In the template tree, right-click a template, and select **New** > **Microsoft Windows/UNIX Remote Server**.
Important information	➤ Enter the actual values for those fields that remain constant throughout the template deployment. Enter template variables in those fields whose values are replaced with a variable value when the template is deployed. For details, see "Referencing Template Variables" on page 957. ➤ You can add only one remote server to a template. This does not apply to templates created in versions of SiteScope earlier than 9.50. ➤ You cannot delete a server from the remote servers list if the server is referenced by a template monitor. Select a different server in the **Server** box of the Monitor Settings pane for each monitor that references the remote server, and then delete the remote server from the remote server list. ➤ You can add a new variable from the New Template Remote Server dialog box by clicking the **New Variable** button, and configuring the variable as described in "New Variable Dialog Box" on page 986. ➤ You cannot replace an existing monitor target server using the Publish Template Changes wizard or auto deployment update (see "Publishing Template Changes Using the XML" on page 1061), although you can change property values of the target server itself, if required. ➤ Do not use "\\" in the remote server **Name** and **Server** fields, and in the monitor **Server** field. ➤ Some fields that contain drop-down lists when configuring objects in normal mode, are displayed as text boxes in template mode.

Relevant tasks	"How to Configure a SiteScope Monitoring Solution Using a Template" on page 964
See also	➤ "Understanding Templates" on page 946 ➤ "Remote Servers Overview" on page 584 ➤ "Template Examples" on page 950 ➤ "Template Tree" on page 95

The following user interface element is common to all areas in the page:

UI Element	Description
New Variable	Click to define a new variable. For details, see "New Variable Dialog Box" on page 986.

For a description of the elements found in the Microsoft Windows New Remote Server dialog box, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603.

For a description of the elements found in the New UNIX Remote Server dialog box, see "New/Edit UNIX Remote Server Dialog Box" on page 610.

New Template Group Dialog Box

This dialog box enables you to add a template group to a template, or to an existing template group to create a subgroup. You use template groups to replicate monitoring deployment to multiple locations in the infrastructure. Template groups are displayed with the icon in the template tree.

To access	Select the **Templates** context. In the template tree, right-click a template or template group, and select **New** > **Group**.
Important information	➤ A template can have only one template group directly under it (the parent group). This does not apply to templates created in versions of SiteScope earlier than 9.50. ➤ By default, you can create template monitors, alerts, and subgroups in the parent group or in subgroups only. If you want to create template monitors directly under a template entity, select the **Allow creation of template monitors directly under template entity** check box in **Preferences** > **Infrastructure Preferences** > **Template Settings**. ➤ You can add a new variable from the New Template Group dialog box by clicking the **New Variable** button, and configuring the variable as described in "New Variable Dialog Box" on page 986.
Relevant tasks	"How to Configure a SiteScope Monitoring Solution Using a Template" on page 964
See also	➤ "Understanding Templates" on page 946 ➤ "Template Examples" on page 950 ➤ "Template Tree" on page 95

The following user interface element is common to all areas in the page:

UI Element	Description
New Variable	Click to define a new variable. For details, see "New Variable Dialog Box" on page 986.

General Settings

User interface elements are described below:

UI Element	Description
Group Name	Name for the template group (preferably using a template variable). A template variable enables you to specify a different name for the group every time you deploy the template. If the group name does not include a variable, multiple deployments of the template in the same directory fail because the group name is not unique. For details on using template variables, see "Referencing Template Variables" on page 957. **Note:** Template deployment fails if a template contains multiple groups with the same name, even if each group has a different parent group.
Group Description	Description for the template group. This can include the most common HTML tags for text styling, such as , <HR>, and <B>, and hyperlinks. The description is displayed only when viewing or editing the group's properties in the SiteScope Dashboard. For details on adding a hyperlink, see "Add URL links to group descriptions - optional" on page 385. **Note:** This field does not support JavaScript/iframes/frames or other advanced features. HTML code entered in this box is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line).

UI Element	Description
Ignore group when publishing changes	(This option is not available for the root group.) Changes made to any objects within this group are ignored when publishing changes to deployed groups. This option enables you to: ➤ Deploy a template inside an existing deployed group and publish template changes to the deployed group without affecting SiteScope objects that are in the ignored group. This means you can edit or delete monitors, groups, or alerts in a deployed group without them being affected when publishing changes. ➤ Delete objects in deployed groups that were removed from the source template (when the **Enable delete on update** option is selected), without deleting other objects created in the deployed group that were not part of the source template. **Default value:** Not selected For the affect of this setting when performing different actions, see the table below.

The following lists the impact of the **Ignore group when publishing changes** setting when different actions are performed:

Action	Effect when Ignore group when publishing changes is selected
Rename Deployed Group	The change of name is ignored by the publish changes flow.
Rename Template Group	
Delete Deployed Group	The group is recreated when you publish changes.
Delete Template Group	The publish changes flow removes the deployed group when **Enable delete on update** is selected.

Action	Effect when Ignore group when publishing changes is selected
Copy a template group	The **Ignore group when publishing changes** setting does not change when copying a template group and its contents to a template.
Copy to a template	The **Ignore group when publishing changes** setting is set to false (cleared) when copying a group and its contents to a template.
Copy between templates	The **Ignore group when publishing changes** setting is copied along with the other template group settings.
Import template from a previous version of SiteScope	The **Ignore group when publishing changes** setting is interpreted as false (cleared).
Export a template	The **Ignore group when publishing changes** setting does not change when exporting a template.

Dependencies

User interface elements are described below:

UI Element	Description
Depends on	Click **Depends on**  to open the Select Depends On Monitor dialog box, and select the monitor on which you want to make the running of this monitor dependent. For details on the Select Depends On Monitor dialog box, see "Select Depends On Monitor Dialog Box" on page 487. 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 value**: No dependency is set for a monitor instance.

UI 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** box reports the condition selected in this box. **Example:** Select Good and this monitor is enabled only when the monitor selected in the **Depends on** box reports a status of Good. The current monitor is automatically disabled if the monitor selected in the **Depends on** box reports a category or condition other than Good. You can also enable dependent monitors specifically for when a monitor detects an error. **Default value:** Good

Search/Filter Tags

Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles).

User interface elements are described below:

UI Element	Description
<Tag name and values>	You can either: ➤ Click the **Add existing tag** button to open the Search/Filter Tags dialog box where you can select an existing tag. For details, see "Search/Filters Tag Dialog Box" on page 1001. ➤ Enter values in the **Tag Name** and **Values** boxes to create new tags. You can also use variables as tags and values. For concept details and for details on how to format the tag names and values, see "Working with Search/Filter Tags" on page 118. The **Tag Name** and **Values** boxes display the selected or entered values. The boxes are empty at first, until you select tags.
Add Existing Tag	Opens the Search/Filters Tag dialog box, enabling you to add existing keyword tags or to define new tags. For user interface details, see "Search/Filters Tag Dialog Box" on page 1001.

New Template Monitor Dialog Box

This dialog box enables you to add a template monitor to a template group or subgroup. Template monitors are used as the basis for the creation of actual monitors at the time that the template is deployed. Template monitors are displayed with the icon in the template tree.

To access	Select the **Templates** context. In the template tree, right-click a template group, and select **New > Monitor**. Select the monitor type you want to configure for the template.

Important information	➤ By default, you create template monitors in a template group. To create template monitors directly under a template entity, select the **Allow creation of template monitors directly under template entity** check box in **Preferences** > **Infrastructure Preferences** > **Template Settings**. Template monitors can contain alerts. ➤ Template monitors are not active monitor instances. Monitors are created and activated based on these template configurations only when you deploy the template. ➤ Do not use "\\" in the monitor **Server** field, and in the remote server **Name** and **Server** fields. ➤ When using regular expressions to select measurement counters or match thresholds, SiteScope checks only whether one string is a substring of another, rather than performing an equality check. This means that the incorrect set of counters and thresholds could be defined in the monitor after deployment. This is because SiteScope, by default, treats every counter in the counters table as a regular expression, and matches the threshold setting with all counters that fit this expression. For example, if the chosen monitor threshold is x/y, and x/yy also matches the regular expression, this threshold is also defined. To avoid this, add specific regular expressions to meet your exact requirements (see "Counter Selection Using Regular Expressions" on page 960). ➤ When adding a Search/Filter tag to a template monitor, you cannot use both actual parameters and variable parameters in the same tag values group. ➤ When deploying a Script monitor from a template, the case of the remote script name must match that of the script name in the scripts subdirectory. Otherwise, the selected script is shown as 'none'. ➤ The Network Bandwidth monitor's non-default thresholds are not copied properly to a template.
Relevant tasks	"How to Configure a SiteScope Monitoring Solution Using a Template" on page 964

See also	➤ "Understanding Templates" on page 946 ➤ "Template Examples" on page 950 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
The settings below are specific to the New Monitor dialog box in template mode only. For settings common to all monitors, see "Common Monitor Settings" on page 447.	
Use already configured template remote under current template	When selecting the server that you want to monitor, enables using the template remote server (if one was created) without having to enter its name. **Default value:** Not selected
New Variable	Opens the New Variable dialog box, which enables you to create a new variable without navigating away from the New Monitor dialog box. For user interface details, see "New Variable Dialog Box" on page 986.

New Alert Dialog Box

This dialog box enables you to define alerts for a template group or a template monitor. Template alerts are used to define alerts on monitors that are created when the template is deployed. If an alert has been set up for the template group or monitor, the alert symbol is displayed next to the group or monitor icon.

To access	Select the **Templates** context. In the template tree, right-click a template group or template monitor, and select **New** > **Alert**.
Important information	You cannot select the **Disable or Enable Monitors** alert action when creating an alert template. Template alerts are enabled for all the monitors belonging to the object for which they were defined. For example, if an alert is defined for a monitor, then it is activated on that monitor only. If an alert is defined for a template, then it is activated for all the monitors in the template.
Relevant tasks	"How to Configure a SiteScope Monitoring Solution Using a Template" on page 964
See also	➤ "Understanding Templates" on page 946 ➤ "SiteScope Alerts Page" on page 1461 ➤ "Template Examples" on page 950 ➤ "Template Tree" on page 95

The following element is common to all action types:

UI Element	Description
New Variable	Click to define a new variable. For details, see "New Variable Dialog Box" on page 986.

For a description of the other elements found in the New Alert dialog box, see "New/Edit Alert Dialog Box" on page 1463.

Search/Filters Tag Dialog Box

This dialog box enables you to select one or more existing tags or to create a new tag.

To access	Click **Add Existing Tag** in the Search/Filters Tag area of template groups, template monitors, and template alerts.
Relevant tasks	"How to Configure a SiteScope Monitoring Solution Using a Template" on page 964
See also	"Search/Filter Tags Overview" on page 904

User interface elements are described below:

UI Element	Description
Add Tag	Click to create a new tag. For details, see "New/Edit Tag Dialog Box" on page 129.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors).
	Represents a tag.

39

Import or Export Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Exporting and Importing Templates

This section provides details about the capability of exporting and importing templates.

You can export templates for use in other SiteScope installations. This enables you to replicate standardized monitor configurations across the enterprise. When you export a template container that includes one or more templates, the template container, and the templates are exported. After exporting, the templates still remain in the template container.

You can also import template configurations from other SiteScope installations. This enables you to efficiently replicate standardized monitor configurations across the enterprise.

For details about the relevant task, see "How to Export and Import a Template" on page 1005.

Tasks

How to Export and Import a Template

This task describes the steps involved in exporting and importing a template.

For details about the relevant concept, see "Exporting and Importing Templates" on page 1004.

This task includes the following steps:

- "Export a template" on page 1005
- "Import a template" on page 1006
- "Result" on page 1006

Note: If the import fails or you no longer see the solution templates in the Solution Templates tree, you can restore them by copying them from the **<SiteScope root directory>\export** folder to the **<SiteScope root directory>\persistency\import** folder. If the **\export** folder also contains the template examples, the template container should be renamed to prevent the unique name violations mentioned above.

---

1 Export a template

Right-click the template container object in the template tree that contains the template or templates you want to export, and click **Export**. Enter the name and location to which you want to save the template file and select the templates to export.

Limitation: When exporting a template without its container, its container is nevertheless exported with the template.

For user interface details, see "Export Template Dialog Box" on page 1008.

2 Import a template

Once you have exported a template, you can copy the export file to another SiteScope server and import the template container that contains the template or templates you want to use. Right-click the template container in the template tree into which you want to import the template or templates, and click **Import**. Enter the name and location of the file you want to import.

For user interface details, see "Import Template Dialog Box" on page 1010.

Note: When importing templates to SiteScope that contain deprecated monitors from earlier version of SiteScope, the deprecated monitors are not displayed in the template tree.

---

3 Result

Templates contained in the file are added to the template container. The imported templates can be used directly or modified as required.

How to Enable Unicode Font When Exporting to a PDF

This task describes how to configure Unicode font to display characters that differ from the current locale when exporting a report to a PDF. This also enables you to view text consisting of characters from multiple languages.

Note: If you are using a machine that has Microsoft Office installed, Arial Unicode MS font is already installed and you do not need to download or configure the font.

To configure Arial Unicode MS font using the font library:

1 Navigate to the font library on the SiteScope server. For example:

Environment	Font Library
AIX	/usr/lpp/Acrobat3/Fonts
HPUX	/usr/contrib/xf86/xterm/fonts /usr/lib/X11/fonts/ms.st/typefaces
Linux	/usr/share/fonts/truetype /usr/share/fonts/local
UNIX	/usr/openwin/lib/X11/fonts/TrueType /usr/X11/lib/X11/fonts/TrueType /usr/X11/lib/X11/fonts/Type1
Windows	C:\Windows\Fonts C:\WINNT\Fonts

2 Download the Arial Unicode MS font into the selected font library. The font is available from http://www.microsoft.com/typography/fonts/family.aspx?FID=24.

3 Restart SiteScope.

Reference

Import or Export Templates User Interface

This section includes:

Export Template Dialog Box

This dialog box enables you to export templates for use in other SiteScope installations. This enables you to replicate standardized monitor configurations across the enterprise. After exporting, the template still remains in the template container.

To access	Select the **Templates** context. In the template tree, right-click the template container object that contains the template or templates you want to export, and select **Export**.
Important information	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. **Limitation:** When exporting a template without its container, its container is nevertheless exported with the template.
Relevant tasks	"How to Export and Import a Template" on page 1005
See also	➤ "Understanding Templates" on page 946 ➤ "Exporting and Importing Templates" on page 1004 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
File Name	**1** Click the **File Name** button to open the Save dialog box where you can browse and select the location where you want to save the file for export. **2** In the **File Name** field in the Save dialog box, enter a name that is descriptive of the template or templates to be exported. **3** Click **Save** to return to the Export Template dialog box. The path and file name you selected are displayed in the **File Name** field in the Export Template dialog box.
Template Tree	Select the templates you want to export. **Default value:** No templates within the template container are selected.

Import Template Dialog Box

This dialog box enables you to import template configurations from other SiteScope installations. This enables you to efficiently replicate standardized monitor configurations across the enterprise.

To access	Select the **Templates** context. In the template tree, right-click the template container into which you want to import the template or templates, and select **Import**.
Relevant tasks	"How to Export and Import a Template" on page 1005
See also	➤ "Understanding Templates" on page 946 ➤ "Exporting and Importing Templates" on page 1004 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
File Name	The name of the template file to be imported. Click the **File Name** button to open the Import Template dialog box from where you can browse and select the location of the file you want to import. After selecting a file, click **Open** to return to the Import Template dialog box. The path and file name you selected are displayed in the **File Name** field.
Override Existing Instances	Select this option if you want templates from the imported file to override existing templates with the same name.

40

Deploy Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Deploy SiteScope Templates Overview

You use templates to rapidly deploy sets of monitors that check systems in the infrastructure that share similar characteristics. After you create and configure templates, you deploy them in the SiteScope hierarchy. After creating a SiteScope monitoring template, you can deploy templates to a group in the following ways:

- You can deploy a single template, or deploy multiple templates simultaneously to a group from the user interface. For task details, see "How to Deploy Templates Using the User Interface" on page 1014.
- You can perform mass deployments of a single template using a CSV file external to the SiteScope user interface. A CSV file is better suited for performing mass deployments, since it is easier to enter and update all the template variable values in one CSV file. For concept details, see "Deploying a Template Using a CSV File" on page 1013. For task details, see "How to Deploy Template Using a CSV File" on page 1017.
- You can deploy a template using an XML file external to the SiteScope user interface. For concept details, see "Auto Template Deployment Overview" on page 1054. For task details, see "How to Deploy a Monitoring Structure Using an XML File" on page 1064.

If you subsequently want to make changes to the source template, you can automatically publish the changes to SiteScope objects deployed by the template using the Publish Template Changes Wizard. For details on updating templates, see "Updating Template Deployments" on page 1032.

Notes and Limitations

- Template deployment fails if a template contains multiple groups with the same name, even if each group has a different parent group.
- Multiple deployments of a template in the same directory fails if the template group name does not include a variable, because the group name is not unique.

Deploying a Template Using a CSV File

After you create and configure templates, you deploy them in the SiteScope hierarchy. You can deploy templates directly from the user interface (see "How to Deploy Templates Using the User Interface" on page 1014), or you can deploy templates from an external Comma Separated Value (CSV) file. The CSV file is used to deploy the variable values defined in the template.

Advantages of using SiteScope CSV template deployment include:

- It is better suited than the user interface for performing mass deployments, since it is easier to enter and update all the template variable values in one CSV file.
- You can perform multiple deployments at one time, without having to manually enter variable values for each deployment in the user interface.
- The template is deployed silently—the template deployment request is submitted to a queue and the deployment is handled in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**.

Note: The maximum queue length for silent deployment is 2000 (each line in a CSV file represents one deployment in the queue).

For details on how to perform this task, see "How to Deploy Template Using a CSV File" on page 1017.

Tasks

How to Deploy Templates Using the User Interface

This task describes the steps involved in deploying SiteScope templates using the user interface.

Tip:

- For mass deployments of a single template, you can also deploy templates using a CSV file. For concept details, see "Deploying a Template Using a CSV File" on page 1013.
- You can also deploy and update the template using an XML file external to the SiteScope user interface. For topic details, see "Auto Template Deployment Overview" on page 1054.

This task includes the following steps:

1 Prerequisites

- Create a SiteScope monitoring template or select an existing user-defined template from the templates tree. For task details, see "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964.
- If you intend to deploy monitors to multiple servers at the same time, you must use a variable as the **Host** value for the template remote server. On deployment, specify multiple server names separated by commas (",") for the host variable.

2 Deploy a single template - optional

a Deploy the template to a group.

- From the monitor tree, right-click the group into which you want to deploy the template, and select **Deploy Template**. In the Select Template dialog box, select the template you want to deploy. For user interface details, see "Select Template Dialog Box" on page 488.
- From the template tree, right-click the template you want to deploy, and select **Deploy Template**. In the Select Group dialog box, select a group into which you want to deploy the template. Alternatively, you can click the **New Group** button and create a new group to which you can deploy the template. For user interface details, see "Select Group Dialog Box" on page 1022.

b In the Deployment Values dialog box, enter the required variable values in the entry boxes displayed. The entry boxes displayed correspond to the template variables used in the template objects. For user interface details, see "Deployment Values Dialog Box" on page 1027.

Example:

If you deploy the **Windows basic template** from the **Template Examples 11.10** folder in the template tree to a SiteScope group, the following entry boxes are displayed in the Deployment Values input window.

3 Deploy multiple templates - optional

a From the template tree, right-click any template container, and select **Deploy Template**. In the Select Group dialog box, select a group into which you want to deploy the templates. Alternatively, you can click the **New Group** button and create a new group to which you can deploy the template. For user interface details, see "Select Group Dialog Box" on page 1022.

b In the Deploy Multiple Templates dialog box, perform the following:

- In the left pane, select the templates that you want to deploy to the group. If you select a template container, all templates within that container are automatically selected.
- In the right pane, enter the required variable values in the entry boxes displayed.
- Below the variable values section in the right pane, configure the permanent options for all the templates being deployed.

For user interface details, see "Deploy Multiple Templates Dialog Box" on page 1024.

4 Results

A summary of the template deployment is displayed. If the deployment is successful, the template objects are added to the monitor tree.

If a template deployment fails, a message displays reasons for the failure. A template monitor might fail to deploy, for example, in the case of a Disk Space monitor, if the disk drive specified in the template does not exist on the deployed server.

How to Deploy Template Using a CSV File

This task describes the steps involved in deploying a SiteScope template using a CSV file.

Tip:

- Alternatively, you can deploy templates using the user interface. For details, see "How to Deploy Templates Using the User Interface" on page 1014.
- You can also deploy and update the template using an XML file external to the SiteScope user interface. For details on this topic, see "Auto Template Deployment Overview" on page 1054.

This task includes the following steps:

1 Prerequisites

- Create a new SiteScope monitoring template or select an existing user-defined or solution template from the templates tree. For task details, see "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964.
- To deploy a solution template using a CSV file, you must first make a copy of the solution template to a template container, and then make the changes required in the steps below to the copied template.

➤ Make sure that the template group name has a unique value in each deployment instance. You can do this by using a variable in the group name, and entering a different variable value in each deployment. You can see an example of this in the **Template Examples 11.10** folder where the group name in **Windows basic template** contains the %%host%% variable.

2 Check the template variable display order

Before creating a CSV file, check the template variable display order for each variable. The column order in the CSV file starts from 0, so make sure the template variable display order also starts from 0 (instead of 1). This is to ensure that the correct columns from the CSV file are mapped to the variables on deployment.

To check the template variable display order:

a Select the **Templates** context. In the template tree, expand the template container that contains the template that you want to deploy using a CSV file, and select the template.

b Select the template variable you want to display first when deploying the template, and check that the **Display order in template** value is 0.

c Repeat for each variable in the template, making sure that the correct display number is used (incremented by 1 each time).

Note: There must be a display order defined for each variable, otherwise the deployment fails.

---

3 Create the CSV File

Open a new text file, and perform the following:

a Enter a variable value for each variable necessary in the deployment, separated by a comma (","). You must be familiar with all the variables defined for the template. Enter values in the order that they are set to be displayed in the **Display order in the template** field (starting from the variable with display order 0).

b Add variable values on a separate line for each deployment instance.

Note:

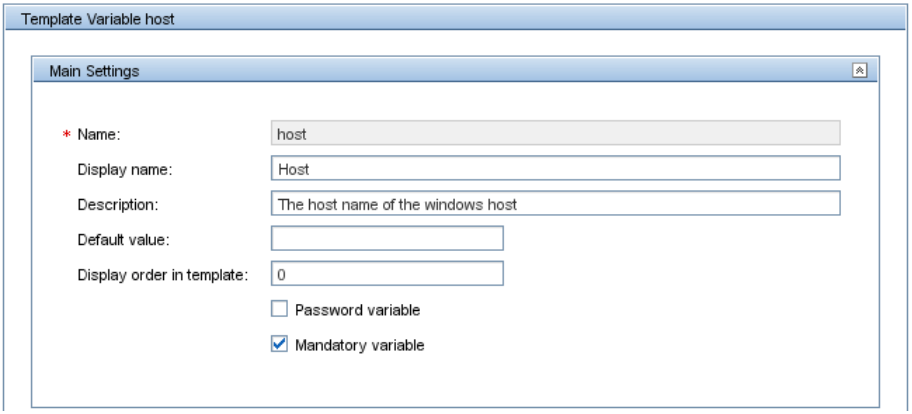
- Spaces are considered part of a field and should not be ignored.
- You do not need to enter non-mandatory variables or default variable values in the CSV file. Instead, you should enter a comma followed by a comma (",,") to represent the variable value.
- When using credentials, we only recommend using a variable for the credential name, since passwords cannot be encrypted in the CSV file.

---

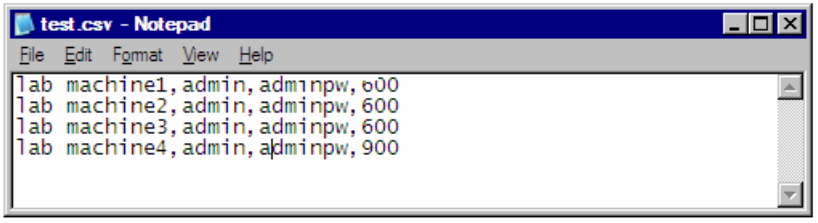
c Save the file in CSV format. After the template is deployed, a group is created for each line in the CSV file.

Example:

To deploy the **Windows basic template** using a CSV file, make sure that the display order for the variables is set as follows: host (0), user (1), password (2), and frequency variables (3). The host template variable settings are displayed below.



Then create a CSV file and enter host, user, password, and frequency values separated by a comma, for each deployment instance (this is the variable display order used in the template).



You do not need to enter a value in the CSV file for the **Frequency** variable (even though it is a mandatory variable), because a default value has been set for this variable in the template (provided you want to use the 600 seconds default value).

4 Deploy the template

a After creating a CSV file for the template, deploy the template to a group.

- From the monitor tree, right-click the group into which you want to deploy the template, and select **Deploy Template Using CSV**. In the Select Template dialog box, select the template you want to deploy. For user interface details, see "Select Template Dialog Box" on page 488.
- From the template tree, right-click the template you want to deploy, and select **Deploy Template Using CSV**. In the Select Group dialog box, select a group into which you want to deploy the template. Alternatively, you can click the **New Group** button and create a new group to which you can deploy the template. For user interface details, see "Select Group Dialog Box" on page 1022.

b In the Select CSV File dialog box, select the CSV file to use for template deployment. For user interface details, see "Select CSV File Box Dialog Box" on page 1029.

5 Results

If the deployment is successful, the template objects are added to the monitor tree. The monitor tree updates itself periodically. Click **Refresh** in the tree toolbar to update the tree and check your deployment.

You can also check the **silent_deployment.log** file for a summary of the deployment. For user interface details, see "Log Files Page" on page 1409.

Note: Typed password values are not displayed in the log file, and instead of the real password, you see a sequence of asterisks ("****").

Reference

Deploy Templates User Interface

This section includes:

- Select Group Dialog Box on page 1022
- Deploy Multiple Templates Dialog Box on page 1024
- Deployment Values Dialog Box on page 1027
- Select CSV File Box Dialog Box on page 1029

Select Group Dialog Box

This dialog box enables you to select a group in the monitor tree to which you can deploy templates. Alternatively, you can select the SiteScope node, and create a new group to which you can deploy templates.

To access	Select the **Templates** context. In the template tree, right-click the template you want to deploy, and select **Deploy Template** or **Deploy Template Using CSV**.
Relevant tasks	➤ "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964 ➤ "How to Publish Template Updates to Related Group Deployments" on page 1035 ➤ "How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Updating Template Deployments" on page 1032 ➤ "SiteScope Solution Templates" on page 1083 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
	Represents the SiteScope root group. You can deploy the templates in the SiteScope root group, or click the **New Group** button and create a new group to which you can deploy the templates.
	Represents a SiteScope monitor group or subgroup (with enabled monitors/with no monitors or no enabled monitors). Select the group to which you want to deploy the templates, or click the **New Group** button and create a new group in which you can deploy the templates.
	Represents the collection of available health monitors that are deployed to check proper functioning of SiteScope monitors.

Deploy Multiple Templates Dialog Box

This dialog box enables you to select multiple templates for deployment to a group simultaneously (instead of deploying each template separately).

To access	Select the **Templates** context. In the template tree, right-click any template container and select **Deploy Template**. In the Select Group dialog box, select the group in which you want to deploy the templates and click **OK**. The Deploy Multiple Templates dialog box opens.
Important information	➤ To deploy monitors to multiple servers at the same time, enter the server names or addresses separated by a comma (","). When doing this, the value in the **Host** property for the template remote server referenced by the monitors must consist of a variable value, and only one variable is allowed. ➤ You can deploy a template, regardless of its content, provided you have edit permissions on the deployment target group. You do not require edit permissions on the template objects such as monitors, remotes, and alerts. ➤ An error message is displayed if a monitor cannot be deployed. This may occur, for example, when deploying the Disk Space monitor template, if the disk drive does not exist on the deployed server.
Relevant tasks	➤ "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964 ➤ "How to Deploy Templates Using the User Interface" on page 1014 ➤ "How to Publish Template Updates to Related Group Deployments" on page 1035
See also	➤ "Updating Template Deployments" on page 1032 ➤ "Template Tree" on page 95

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element	Description
Select Templates (left pane)	
<template tree>	Select the templates that you want to deploy from the template tree. ➤ When you select a template container, all templates within that container are selected. If you select the SiteScope root, all templates in the template tree are selected. ➤ The ▣ icon displayed to the left of the SiteScope root or a template container indicates that not all templates within SiteScope or the specific container have been selected.
Template Deployment Settings (right pane)	
<template variable values>	A list of variables used in each selected template is displayed under a label with the full path of the corresponding template in the right pane. Enter deployment values for the variables (variables that are mandatory are denoted by a red asterisk).
Silent deployment	Submits the template deployment request to a queue. SiteScope handles the deployment in the background, enabling you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected

UI Element	Description
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in each template against the remote servers on which the templates are being deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected
Test remote servers	Tests the connection created from the template remote servers after the templates have been deployed. The test is performed in the background, enabling you to continue to use SiteScope. **Default value:** Not selected

Deployment Values Dialog Box

This dialog box enables you to enter variable values when deploying the template.

To access	Select the **Templates** context. In the template tree, right-click the template that you want to deploy (it must contain variables), and select **Deploy Template**. In the Select Group dialog box, select the group in which you want to deploy the template and click **OK**. The Deployment Values dialog box opens.
Important information	➤ To deploy monitors to multiple servers at the same time, enter the server names or addresses separated by a comma (","). When doing this, the value in the **Host** property for the template remote server referenced by the monitors must consist of a variable value, and only one variable is allowed. ➤ You can deploy a template, regardless of its content, provided you have edit permissions on the deployment target group. You do not require edit permissions on the template objects such as monitors, remotes, and alerts. ➤ An error message is displayed if a monitor cannot be deployed. This may occur, for example, when deploying the Disk Space monitor template, if the disk drive does not exist on the deployed server.
Relevant tasks	➤ "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964 ➤ "How to Deploy Templates Using the User Interface" on page 1014 ➤ "How to Publish Template Updates to Related Group Deployments" on page 1035
See also	➤ "Updating Template Deployments" on page 1032 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
<variable name>	Each variable that is referenced in a template object prompts the display of a corresponding entry box when the template is deployed. The variable name is used as a label for the text entry box. Enter deployment values for the variables.
Silent deployment	Submits the template deployment request to a queue, and have SiteScope handle the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is being deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected
Test remote servers	Tests the connection created from the template remote server after the template has been deployed. The test is performed in the background, enabling you to continue to use SiteScope. **Note:** This option is displayed only when deploying a template that includes a remote server. **Default value:** Not selected

Select CSV File Box Dialog Box

This dialog box enables you to select the CSV file to use when deploying a template.

To access	Use one of the following: ➤ Open the **Templates** context. In the template tree, right-click the template you want to deploy, and select **Deploy Template Using CSV**. In the Select Group dialog box, select the group to which you can deploy the template, and click **OK**. ➤ Open the **Monitors** context. In the monitor tree, right-click the group to which you want to deploy the template, and select **Deploy Template Using CSV**. In the Select Template dialog box, select the template that you want to deploy, and click **OK**.
Relevant tasks	➤ "How to Configure a SiteScope Monitoring Solution Using a Template" on page 964 ➤ "How to Deploy Template Using a CSV File" on page 1017
See also	➤ "Updating Template Deployments" on page 1032 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
CSV file	Comma Separated Values (CSV) file to use for deploying the variable values defined in the template. Click the **Select** button, and select a CSV file to use for the template deployment. **Note:** You can only use a file with a CVS extension.
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected
Test remote servers	Tests the connection to the template remote server after the template has been deployed. The test is performed in the background, enabling you to continue to use SiteScope. **Note:** This option is displayed only when deploying a template that includes a remote server. **Default value:** Not selected

41

Publish User-Defined Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Updating Template Deployments

You can make changes to the template, and publish the changes to all SiteScope objects deployed by the template using the Publish Template Changes Wizard. If a change is required to a template object, for example, a threshold value changes or a new monitor or alert is required, you can update the template once and publish the changes to all deployed groups without having to update each object individually.

You can also view how the actual monitored deployments comply with the standardized deployment as defined in the source template using the Publish Template Changes Wizard. This ensures that any changes in the monitored environment can be quickly updated in the monitoring infrastructure and that the monitoring infrastructure is still compliant with the standards set in the source template.

Note: You can run the Publish Template Changes Wizard provided you have **Edit groups** permissions, and only on groups for which you have permissions in the **Allowed groups** list. Any deployed groups that are not in your allowed groups list are not displayed in the wizard.

When you deploy a template, the deployed parent group is automatically associated to the source template. If you subsequently make changes to the source template, you can automatically publish the changes to SiteScope objects deployed by the template using the Publish Template Changes Wizard. The wizard enables you to update related deployed groups across the enterprise whenever the source template is updated without having to update each object individually.

A deployed group consists of the groups, monitors, alerts, variables, and the remote server configured in the template. For details on how to deploy a template, see "Deploy the template" on page 971.

The Publish Template Changes Wizard enables you to update deployed groups in the following ways:

- You can publish only the changes in the source template to the deployed groups. This would create added objects and update values of existing objects, but leave other objects not in the source template intact.
- You can publish the changes in the source template to the deployed groups and have SiteScope make the above changes and delete all other SiteScope objects that are not in the source template from the deployed groups.
- When publishing changes, you can have SiteScope ignore publishing changes to groups under the root group. This enables:
  - Deploying a template inside an existing deployed group and publishing template changes to the deployed group without affecting SiteScope objects that are in the ignored group. This enables deploying templates inside different deployed groups.
  - Deleting objects in deployed groups that were removed from the source template (when the **Enable delete on update option** is selected), without removing other objects created in the deployed group that were not part of the source template.

For details on how to publish template changes, see "How to Publish Template Updates to Related Group Deployments" on page 1035.

For details on the Publish Template Changes Wizard user interface, see "Publish Template Changes Wizard" on page 1040.

Notes and Limitations

- If you are using groups deployed by templates created in versions of SiteScope earlier than 9.50, root groups are not associated with the source template. You can update these template deployments using the following methods:
  - Manually associate the template groups with the source template using Global Search and Replace.
  - Enter the path of the source template in the **Source template** box in the General Settings for the current group.

- Templates and deployed groups are internally linked by an ID. This means that you can publish changes even if the name of the template or the root group in a deployed group have changed. However, if you manually associate a group to a template using the **Source template** property of the root group, you cannot publish changes if the root group name was changed in the deployment.
- For changes to be published, all changes in the root group hierarchy must succeed. If any changes to a group fail, all changes to that group are rolled back.
- Changes to Search/Filter tag values are not shown in the Review Compliancy page of the Publish Template Changes Wizard. However, the changes are published to the deployed group.
- The Publish Template Changes Wizard does not support regular expressions in threshold settings.
- The Publish Template Changes Summary report PDF is not supported in Firefox 2.x.
- For characters to be displayed in most languages when exporting a report to a PDF, Arial Unicode MS font must be installed on the machine used to view the PDF. For details, see "How to Enable Unicode Font When Exporting to a PDF" on page 1007.
- Properties are displayed in the Publish Template Changes Wizard according to the locale of the server where SiteScope is installed. The browser locale has no effect on how the properties are displayed.
- You cannot replace an existing monitor target server using the Publish Template Changes wizard or auto deployment update (see "Publishing Template Changes Using the XML" on page 1061), although you can change property values of the target server itself, if required.
- To publish changes in browsable monitor counters to deployed groups, there must be a connection to the remote server on which the monitor groups are deployed.
- You can also use the SiteScope API to update groups, monitors, alerts, and remote servers deployed by a template. For details, see "Using the SiteScope Configuration API" on page 42.

Tasks

How to Publish Template Updates to Related Group Deployments

This task describes the steps involved in publishing template changes to related group deployments using the Publish Template Changes Wizard.

This task includes the following steps:

- "Run the Wizard" on page 1036
- "View the structural and content differences" on page 1037
- "Add new variable values" on page 1038
- "Review the publish template changes results" on page 1039
- "Export the template changes to a summary report - optional" on page 1039

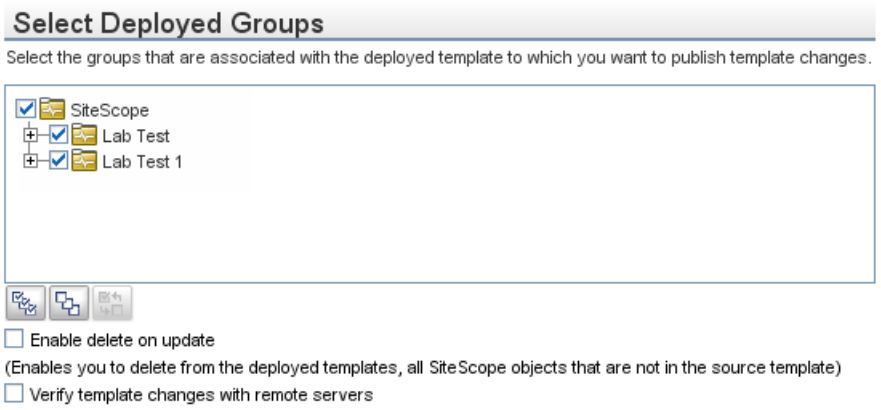
1 Run the Wizard

In the template tree, right-click a template, and select **Publish Changes** to run the wizard. On the first page, select the related template groups that you want to update. You can also select the following options:

- **Enable delete on update** to delete SiteScope objects from the deployed groups that are not in the source template.
- **Verify template changes with remote servers** to verify the correctness of the monitor configuration changes in the selected template with the remote servers on which the template is deployed.

For user interface details, see "Publish Template Changes Wizard" on page 1040.

Example:

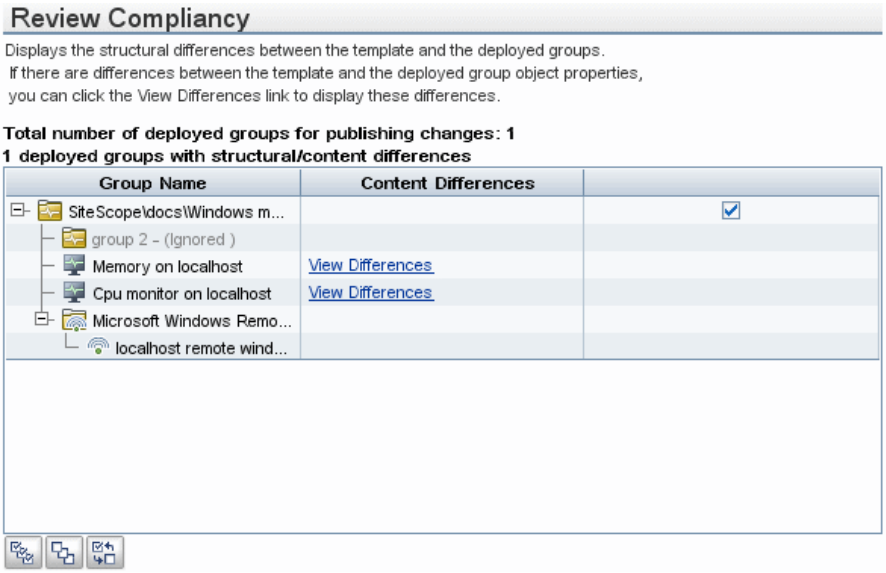


2 View the structural and content differences

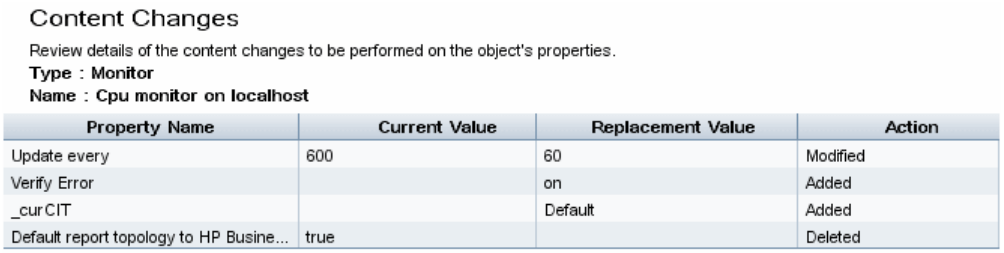
View the structural differences between the template and the deployed groups. For details on the Review Compliancy user interface, see "Review Compliancy Page" on page 1043.

To view content differences in the template objects, click the **View Differences** link to open the Content Changes dialog box. This link appears only for template objects that have content differences. For details on the Content Changes user interface, see "Content Changes Dialog Box" on page 1045.

Example - Review Compliancy Page:



Example - Content Changes Page:

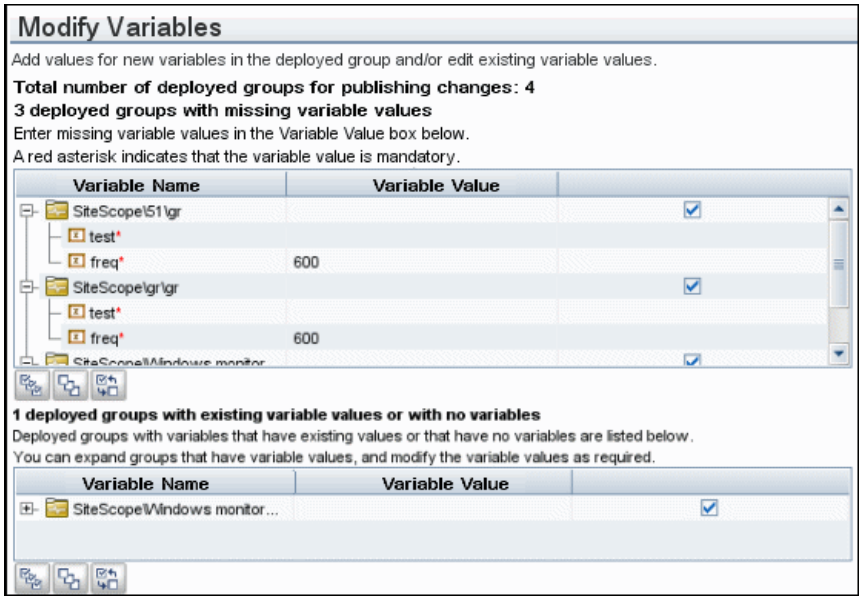


3 Add new variable values

Add values for any new variables in the template. Variable values that are mandatory are indicated by a red asterisk (*). You can also edit values of existing variables. Click **Apply** to complete the wizard and publish the template updates.

For user interface details, see "Modify Variables Page" on page 1046.

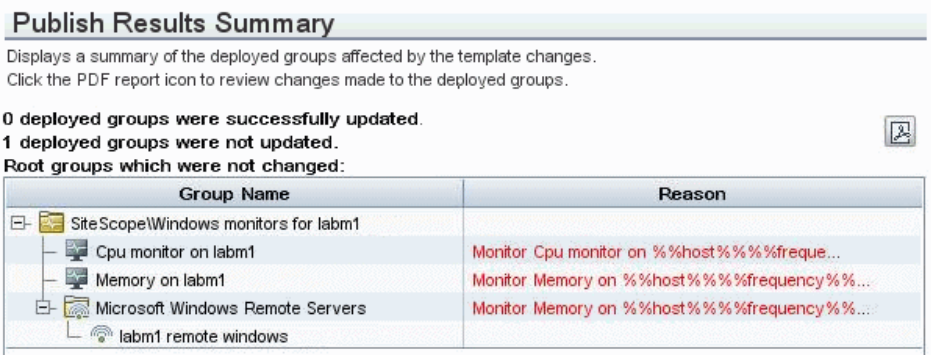
Example - Modify Variables Page:



4 Review the publish template changes results

Review the results of the publish template changes and, if necessary, retry publishing the changes to the deployed groups that failed to update. For details on the Publish Results Summary user interface, see "Publish Results Summary Page" on page 1047.

Example - Publish Results Summary Page:



5 Export the template changes to a summary report - optional

Optionally, you can export the publish template change results to a summary report (PDF file). For details on the summary report, see "Publish Template Changes Summary Report" on page 1049.

Reference

Publish Template Changes Wizard

This wizard enables you to check deployed groups for template compliancy and to update SiteScope objects deployed by templates whenever the source template is updated.

To access	Select the **Templates** context. In the template tree, right-click a template, and select **Publish Changes**.
Important information	➤ You can run the Publish Template Changes Wizard provided you have **Edit groups** permissions, and only on groups for which you have permissions in the **Allowed groups** list. Any deployed groups that are not in your allowed groups list are not displayed in the wizard. ➤ The wizard opens only if there are deployments associated with the selected template. For details on deploying templates, see "Deploy the template" on page 971.
Relevant tasks	"How to Publish Template Updates to Related Group Deployments" on page 1035
Wizard map	This wizard contains: Select Deployed Groups Page > Review Compliancy Page > Content Changes Dialog Box > Modify Variables Page > Publish Results Summary Page > (Publish Template Changes Summary Report)
See also	➤ "Updating Template Deployments" on page 1032 ➤ "Template Tree" on page 95

Select Deployed Groups Page

This wizard page enables you to select groups associated with the source template for which you want to apply template changes.

Important information	General information about this wizard is available here: "Publish Template Changes Wizard" on page 1040.
Wizard map	The Publish Template Changes Wizard contains: **Select Deployed Groups Page** > Review Compliancy Page > Content Changes Dialog Box > Modify Variables Page > Publish Results Summary Page > (Publish Template Changes Summary Report)
See also	➤ "Updating Template Deployments" on page 1032 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
<List of groups associated with the selected template>	Groups associated with the selected template that you want to update with the template changes. **Default value:** All associated groups and subgroups are selected.

UI Element	Description
Enable delete on update	Select this option to ensure template compliancy. Deletes all SiteScope objects that are not in the source template from the deployed groups, except for objects in groups under the root group where the **Ignore group when publishing changes** option is selected. For details on the ignore group setting, see "New Template Group Dialog Box" on page 991. **Note:** Template groups with the **Ignore group when publishing changes** option selected that were deployed and then removed from the template are removed from the deployment after publishing changes with **Enable delete on update** selected. **Default value:** Not selected
Verify template changes with remote servers	Verifies the correctness of the monitor configuration changes in the selected template with the remote servers on which the template is deployed. **Note:** Selecting this option slows update performance time due to the remote connection. **Default value:** Not selected

Review Compliancy Page

This wizard page enables you to view the structural differences between the source template and the deployed groups, and provides links to content differences in the deployed group objects.

Important information	➤ General information about this wizard is available here: "Publish Template Changes Wizard" on page 1040. ➤ Changes to Search/Filter tag values are not shown in the Review Compliancy page of the Publish Template Changes Wizard. However, they are published to the deployed group.
Wizard map	The Publish Template Changes Wizard contains: Publish Template Changes Wizard > **Review Compliancy Page** > (Content Changes Dialog Box) > Modify Variables Page > Publish Results Summary Page > (Publish Template Changes Summary Report)
See also	"Updating Template Deployments" on page 1032

User interface elements are described below:

UI Element	Description
<N> deployed groups with structural/ content differences	Displays the deployed groups and group objects (subgroups, monitors, alerts, and remote servers) that have structural or content differences to the source template.
<N> deployed groups with no structural/ content differences	Displays the deployed groups that have no structural or content differences to the source template. Groups with no deployment differences are displayed collapsed.

UI Element	Description
Group Name	Displays the name of the deployed group and all its objects—subgroups, monitors, alerts, alert actions, and remote servers. Structural differences in the objects are displayed in the group tree hierarchy with the following text and color coding: ➤ **Added.** Indicates a new object to be added to the deployed group. The object is displayed in green. ➤ **Does not exist in template** (available only when the **Enable delete on update** option is not selected in the Select Deployed Groups). Indicates an object that does not exist in the source template. The object is displayed in blue. ➤ **Ignored.** Indicates a sub-group that has the **Ignore group when publishing changes** option selected. Ignored groups are displayed in gray. ➤ **Removed** (available only when the **Enable delete on update** option is selected in the Select Deployed Groups). Indicates an object to be deleted from the deployed group. The object is displayed in red. ➤ **Unused.** Indicates that the template remote server is not being used. An unused remote server is displayed in gray.
Content Differences	For objects that contain content differences in properties, thresholds, and any other non-structural differences, the **View Differences** link is displayed. Click the link to open the Content Changes dialog box and view differences in the property level for the deployed group or object. For user interface details, see "Content Changes Dialog Box" on page 1045. Template remote servers that have been deployed are displayed in the **Microsoft Windows Remote Servers** or **UNIX Remote Servers** section. If a remote server already exists in Microsoft Windows/UNIX Remote Servers, it is not deployed again when the template is deployed.

Content Changes Dialog Box

This wizard page enables you to view a list of all properties of the selected object to be updated, the current and the replacement values, and the property action status.

Important information	General information about this wizard is available here: "Publish Template Changes Wizard" on page 1040.
Wizard map	The Publish Template Changes Wizard contains: Publish Template Changes Wizard > Review Compliancy Page > (**Content Changes Dialog Box**) > Modify Variables Page > Publish Results Summary Page > (Publish Template Changes Summary Report)
See also	"Updating Template Deployments" on page 1032

User interface elements are described below:

UI Element	Description
Type	Object type (Group, Monitor, Alert, Alert Action, Remote).
Name	Name of the selected object.
Property Name	Name of the property affected by publishing the change.
Current Value	Existing property value in the deployed group. This value is empty if the property is going to be added to the deployed group. **Note:** Existing password properties are displayed encrypted.

UI Element	Description
Replacement Value	Replacement property value in the template. This value is empty if the property is going to be deleted from the deployed group. **Note:** ➤ Replacement password properties are displayed encrypted. ➤ If you make changes to the **Depends on** property in a template monitor, the full path of the template monitor to which there is a dependence is displayed (for example, SiteScope\tc\template\group\CPU).
Action	Status of the action (Modified, Added, Deleted, Ignored). Ignored status is used for baseline monitors, if there are no changes to the baseline thresholds.

Modify Variables Page

This wizard page enables you to add values for new variables in the deployed group. You can also edit existing variable values.

Important information	General information about this wizard is available here: "Publish Template Changes Wizard" on page 1040.
Wizard map	The Publish Template Changes Wizard contains: Publish Template Changes Wizard > Review Compliancy Page > (Content Changes Dialog Box) > **Modify Variables Page** > Publish Results Summary Page > (Publish Template Changes Summary Report)
See also	"Updating Template Deployments" on page 1032

User interface elements are described below:

UI Element	Description
Variable Name	Name of a new or existing variable in the deployed group. A red asterisk indicates that the variable value is mandatory. **Note:** You can expand groups with variable values already filled, and modify the variables as required. You cannot expand groups that do not contain variables.
Variable Value	Value for new variables added to the deployed group. You can also edit existing variable values. **Note:** ➤ The variable value for the remote server is read only and cannot be changed. ➤ Hypertext tags in a variable string cause the string to be truncated and be incorrectly displayed in the Variable Value box (part of the string is displayed in the text label).

Publish Results Summary Page

This wizard page enables you to view a summary of the published template updates.

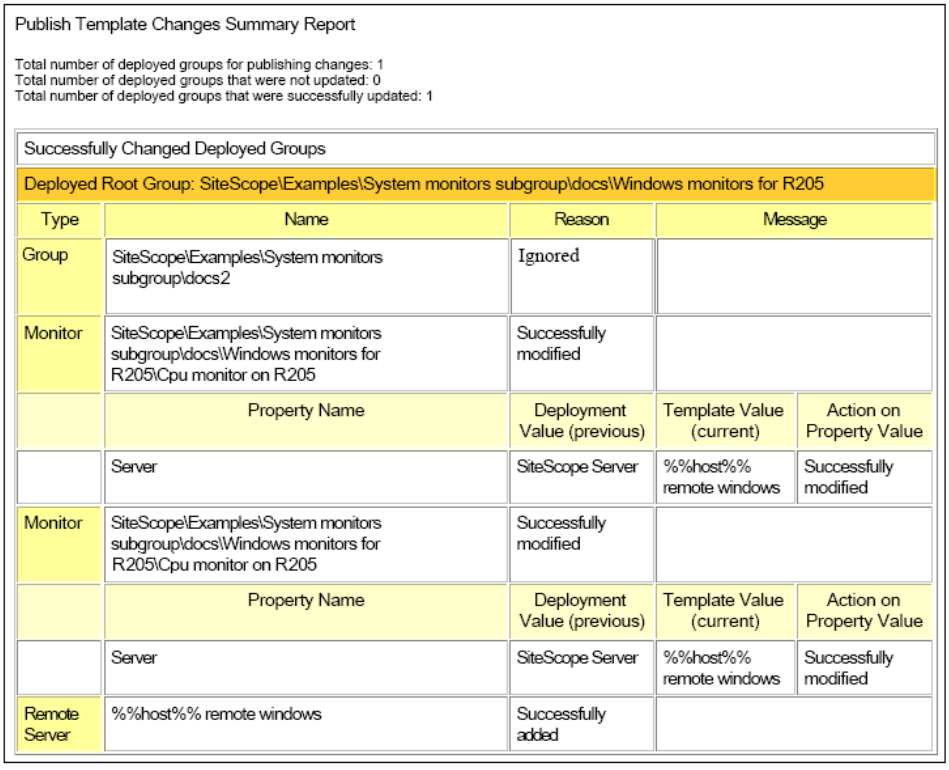
Important information	General information about this wizard is available here: "Publish Template Changes Wizard" on page 1040.
Wizard map	The Publish Template Changes Wizard contains: Publish Template Changes Wizard > Review Compliancy Page > (Content Changes Dialog Box) > Modify Variables Page > **Publish Results Summary Page** > (Publish Template Changes Summary Report)
See also	"Updating Template Deployments" on page 1032

User interface elements are described below:

UI Element	Description
	**Export.** Exports the results of publishing for each root group to a PDF file. For details, see "Publish Template Changes Summary Report" on page 1049.
Group Name	Displays the root group name and the group's objects (subgroups and monitors).
Reason	If SiteScope is unable to publish changes to a deployed group, the reason for failure is displayed for each monitor in the group.

Publish Template Changes Summary Report

This report displays information about the template changes published to the deployed groups. It also displays information for group objects that failed to update or that were ignored. Results are at the object level (Group, Monitor, Alert, Alert Action, Remote Server).



Publish Template Changes Summary Report

Total number of deployed groups for publishing changes: 1
Total number of deployed groups that were not updated: 0
Total number of deployed groups that were successfully updated: 1

Successfully Changed Deployed Groups				
Deployed Root Group: SiteScope\Examples\System monitors subgroup\docs\Windows monitors for R205				
Type	Name	Reason	Message	
Group	SiteScope\Examples\System monitors subgroup\docs2	Ignored		
Monitor	SiteScope\Examples\System monitors subgroup\docs\Windows monitors for R205\Cpu monitor on R205	Successfully modified		
	Property Name	Deployment Value (previous)	Template Value (current)	Action on Property Value
	Server	SiteScope Server	%%host%% remote windows	Successfully modified
Monitor	SiteScope\Examples\System monitors subgroup\docs\Windows monitors for R205\Cpu monitor on R205	Successfully modified		
	Property Name	Deployment Value (previous)	Template Value (current)	Action on Property Value
	Server	SiteScope Server	%%host%% remote windows	Successfully modified
Remote Server	%%host%% remote windows	Successfully added		

To access	In the Publish Results Summary Page of the Publish Template Changes wizard, click the **Report**  button.
Important information	➤ General information about this wizard is available here: "Publish Template Changes Wizard" on page 1040. ➤ The Publish Template Changes Summary Report PDF is not supported in Firefox 2.x. ➤ For characters to be displayed in most languages when exporting a report to a PDF, Arial Unicode MS font must be installed on the machine used to view the PDF. For details, see "How to Enable Unicode Font When Exporting to a PDF" on page 1007.
Relevant tasks	"How to Publish Template Updates to Related Group Deployments" on page 1035
Wizard map	The Publish Template Changes Wizard contains: Publish Template Changes Wizard > Review Compliancy Page > (Content Changes Dialog Box) > Modify Variables Page > Publish Results Summary Page > (**Publish Template Changes Summary Report**)
See also	"Updating Template Deployments" on page 1032

Report Content

User interface elements are described below:

UI Element	Description
<Report summary>	Total number of root groups selected for publishing changes, including the number of groups that were successfully and unsuccessfully changed.
Deployed Root Group <group path>	Name of the deployed group and all group objects that were successfully or unsuccessfully updated with the template changes. The deployed groups that were not updated are displayed first. **Note:** For changes to be published, all changes in the root group hierarchy must succeed. If any changes to a group object fail, all changes to that group are rolled back.
Type	Object type (Group, Monitor, Alert, Alert Action, Remote Server).
Name	Name of the object and its path.
Reason	Publish status for the object (Successfully added, Successfully modified, Successfully deleted, Failed to add, Failed to modify, Failed to delete, Ignored, Unchanged).

UI Element	Description
Message	For deployed group objects that were not updated by the template changes, the reason for the failure to publish the changes.
<Property details>	For deployed group objects that had content changes: ➤ **Property Name.** The name of the property that was updated. ➤ **Deployment Value (previous).** The previous property value in the deployed group. This value is empty for a property that was added to the deployed group. Previous password variables are displayed encrypted. ➤ **Template Value (current).** The replacement property value in the deployed group. This is the current property value in the template. This value is empty if the property was deleted from the deployed group. Replacement password variables are displayed decrypted. ➤ **Action on Property Value.** The type of change made to the property value (Successfully modified, Successfully added, Successfully deleted).

42

Auto Template Deployment

This chapter includes:

Concepts

Tasks

Reference

Concepts

Auto Template Deployment Overview

SiteScope enables you to automatically deploy a SiteScope template or solution template using an XML file external to the SiteScope user interface. The XML file is used to deploy the objects defined in the template, which must include a parent group and can include subgroups, monitors, a remote server, alerts, and variable definitions. You can edit the XML file to assign variable definitions for mandatory, global, and instance variables.

For details on creating templates, see "SiteScope Templates Overview" on page 944. For details on working with solution templates, see "Solution Templates Overview" on page 1084.

You can also use the auto template deployment to publish template changes to deployed groups. The auto template deployment uses the same functionality as the Publish Template Changes Wizard. For details on how the wizard works, see "Updating Template Deployments" on page 1032.

Auto template deployment is an alternative to using the user interface to deploy templates and publish template changes to deployed groups. It is better suited than the user interface for working with scripts and deploying onto multiple SiteScopes. This is because it uses standard XML scripting and can be deployed onto multiple SiteScopes using one file.

Creating and Working with the XML File

Use one of the following options to create the XML file:

- Generate and edit your XML in any tool that supports text. The file must be based on the XSD file supplied in the SiteScope file directory. The XSD file is a basic XML file which already includes the appropriate tags, elements, and attributes for creating your own version of the deployment XML.
- Generate the deployment XML file using the SiteScope interface from a template container or solution template. Each template container and solution template includes the option to generate this auto template deployment XML file. For details, see "Generate Auto Deployment XML User Interface" on page 1075.

The XML you use, whether generated from the template or solution template, or generated manually, must be a valid XML and match the ATD schema (XSD). You can use the dedicated tool to validate your XML file.

Deploying the XML file is dependent on the target SiteScope having the relevant template or solution template in its monitor tree. You deploy the template or solution template by copying the XML file into the persistency folder of the target SiteScope with the relevant template or solution template. You can group several deployments into a single XML file.

XML File Example and Variables

For a reference detailing all the XML tags, elements, and attributes included in the auto template deployment file, see "XML Tag Reference" on page 1071.

Each auto template deployment XML must begin with the following declarations:

- **<?xml version="1.0" encoding="UTF-8" ?>** This states that this is an XML with UTF-8 character encoding.
- **<sitescope:sitescopeRoot …>** This is the schema declaration. Despite the URLs mentioned, this does not try to connect to any location outside of your SiteScope at any time.

Each section of the XML file begins with one of the following tags, with the instruction to perform one of the following actions:

- **<sitescope:templateDeployment>** Deploys a template or solution template. You can have multiple instances within the same XML file.
- **<sitescope:templateDeployUpdate>** Publishes changes to an existing deployment.

Within each action, you must specify the following:

- **<deploy:fullPathtoTemplate>** The path to the template within the SiteScope tree in the user interface, not including the SiteScope root node. In the XML file example, this value is Templates/Windows.
- **<deploy:fullPathToDestinationGroup>** The path, within the SiteScope tree, of the target group on which the action is performed. For example, in the XML file example, any template group objects are created as subgroups within the following group SiteScope/Windows_Monitors.

This section contains the following topics:

- "XML File Example" on page 1057
- "Variables" on page 1058

XML File Example

Here is an example of the auto template deployment XML file. This file was generated from the user interface.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--SiteScope deployment descriptor-->
<sitescope:sitescopeRoot xmlns:sitescope="./sitescope" xmlns:deploy="./deploy"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="./sitescope
../schemas/sitescope.xsd ">
    <!--To deploy use "templateDeployment", to update an existing deployment use templateDeploymentUpdate
(this element can have the attribute enableDeleteOnUpdate with values of yes/no)-->
    <sitescope:templateDeployment>
        <!--Path to source template in SiteScope tree (not including the root node)-->
        <deploy:fullPathToTemplate>Template Examples/Windows basic template
</deploy:fullPathToTemplate>
        <!--Path to destination group in SiteScope tree (not including the root node). New group will be
created if need be-->
        <deploy:fullPathToDestinationGroup> </deploy:fullPathToDestinationGroup>
        <deploy:login user="admin99" password="(sisp)n9JRVALxlsq="/>
        <!--Mandatory variables names-->
        <deploy:mandatoryFields>host frequency password user</deploy:mandatoryFields>
        <!--Global values for variables in current template-->
        <deploy:globalVariables>
            <deploy:variables encrypted="no" name="frequency" value="600"/>
            <deploy:variables encrypted="no" name="password" value="(sisp)d5JLOSWaVfe="/>
            <deploy:variables encrypted="no" name="user" value="admin"/>
        </deploy:globalVariables>
        <!--Add here local variables for a deploy instance (overrides global variables with same name)-->
        <deploy:templateInstanceDeployVariable>
            <deploy:variables encrypted="no" name="group" value="Critical_monitors"/>
            <deploy:variables encrypted="no" name="frequency" value="600"/>
        </deploy:templateInstanceDeployVariable>
        <deploy:templateInstanceDeployVariable connectToServer="no">
            <deploy:variables encrypted="no" name="group" value="Minor_monitors"/>
            <deploy:variables encrypted="no" name="frequency" value="6000"/>
        </deploy:templateInstanceDeployVariable>
    </sitescope:templateDeployment>
</sitescope:sitescopeRoot>
```

Variables

After the template and destination have been specified, the next section of the XML file deals with the template variables and values. The XML file gives you the flexibility of defining variables and their values, declaring mandatory variables, and determining if their corresponding values should be applied globally across the deployment or per instance.

If you generated the XML file from the user interface and if a variable has a defined value, that value is assigned to the variable in the XML file.

Mandatory Variables

A declaration of any mandatory variables in the template appears in the **<deploy:mandatoryFields>** tag. If a variable is declared mandatory, a corresponding value for the variable must be defined in the in the file.

If you generated the XML from the user interface and if the **Mandatory** option was selected when creating or editing a variable, that variable appears in the **<deploy:mandatoryFields>** tag. You can also manually add a variable name to this list to declare it mandatory.

In the file example above, group and frequency have been defined as mandatory variables. Values for these variables must appear within the **<deploy:variables>** tags for either the **<deploy:globalVariables>** or the **<deploy:templateInstanceDeployVariables>**.

Global Variables or Instance Variables

The optional **<deploy:globalVariables>** tag includes the default global template variables for the deployment. Defining global template variables is optional. When you define a global template variable, you can overwrite the variable's value by identifying a different variable value in the deployment instance area of the file (**<templateInstanceDeployVariables>** tag). Global variable values can be overwritten with a different value in each deployment instance.

Multiple instances of a template that are deployed into the same location onto the same SiteScope, as seen in the XML file example, must include a variable for the group name. Group name must be made a mandatory variable and given a different value in each deployment instance. The group template object must have the same variable defined as its value. The template could include other groups whose name value is not a variable and those groups would be deployed once.

In the XML file example above, there are two instances of the deployment, so a variable called group has been defined as mandatory and a different value has been given to it in each instance deployment (Critical_monitors and Minor_monitors). This results in two groups created under the group object of the template with the same monitor objects.

The following groups would result from the XML file example being deployed:

- SiteScope/Windows_Monitors/Critical_monitors in the first instance of the deployment.

  Included in this group would be any monitors and alerts defined in the template. Any of the template monitor objects whose frequency value was defined as the variable frequency would have a value of 600 (every 10 minutes).

- SiteScope/Windows_Monitors/Minor_monitors in the second instance of the deployment.

  Included in this group would be any monitors and alerts defined in the template. Any of the template monitor objects whose frequency value was defined as the variable frequency would have a value of 6000 (every hour). The connectToServer="no" attribute was added to this group. This means that the monitor configuration properties in the template will not be verified against the remote server on which the template is deployed.

The XML file example also contains a login with a user name and password (<deploy:login user="admin99" password="(sisp)n9JRVALxIsq=" />). It is mandatory to specify a valid user name and password for each deployment when using a secure environment. You can use the encryption tool to encypt the user name and password.

Note: If you have any system variables defined in a template (those defined by $$ and not %%), they are treated as normal variables in the auto template deployment XML file. The same limitations that apply to using system variables in templates apply to using them in the XML file.

XML Validator

The XML validator is a utility that validates the XML file against the schemas used by the auto template deployment. It does not validate the SiteScope deployment itself. The path to the validator file is:

- For Windows: **<SiteScope root directory>/tools/AutoDeployment/validate_template_xml.bat**
- For UNIX: **<SiteScope root directory>/tools/AutoDeployment/validate_template_xml.sh**

This utility checks the structure of the XML against the XSD files to make sure that the contents of the file are valid XML and correspond to the XSD. It also validates that there have been values defined for all mandatory variables. The values can be defined either as global variables or deployment instance variables. If the validation fails, the reason for the failure is printed to screen.

Publishing Template Changes Using the XML

You can also use the auto template deployment XML to publish template changes to update the values or structure of a deployed group. If the group's **Source Template** field is identified as the same template that the XML is referencing, you can update the values and objects of the group using the auto template deployment XML.

The XML uses the same functionality as the Publish Template Changes Wizard but without having to access the user interface. In the XML file, you can identify values for variables to use for publishing the changes in the template. For details on the wizard and the template update feature, see "Updating Template Deployments" on page 1032.

You can use auto template deployment to publish the changes made to a template onto the template's deployed groups in the same way you use the XML to create a group deployment. After the template has been modified, you create the XML and copy/paste the edited XML into the persistency folder of the target SiteScope machines.

This section also includes:

Update Deployment XML Tag Details

The XML file for updating the values or objects of a deployed group must use the <**sitescope:templateDeploymentUpdate**> tag (and not the <**sitescope:templateDeployment**> tag used for deploying the template). For details on the elements and attributes to use in the XML file, see "XML Tag Reference" on page 1071.

Within the <**sitescope:templateDeploymentUpdate**> tag, you can select to give the **enableDeleteOnUpdate** attribute a value of **yes** to make sure that any objects within the deployed groups that do not appear in the template referenced by the auto template deployment XML are deleted when updating the deployment with the XML file. Enter a value of **no** to make sure that all objects within the group are retained, even if they do not appear in the template referenced by the XML file, after the updating the deployment. For details on this option in the Publish Template Changes Wizard, see "Enable delete on update" on page 1042.

To successfully perform the update, you must define the target SiteScope group name of the deployed group as the value of the **deploy:fullPathToDestinationGroup** tag. The **fullPathToDestination** must end with the root group of the deployment, the equivalent of the template's root group. Each deployment section updates one group so if you have multiple groups, you must define separate deployment update sections for each and define the group name for each.

Template Update Report

After performing the auto template deployment update, a report is available in XML format. The report file is named with the name of the XML file along with a time stamp and the string **_reports**. These reports are available in the following location: <**SiteScope root directory**>**persistency****autodeployment****reports**.

The report is in XML format and includes the following tags at the beginning:

- **totalNumberOfDeployments**
- **totalNumberOfFailedDeployments**
- **totalNumberOfSuccessDeployments**

The **<publishChangesSummaryPage>** section of the XML appears for each deployment instance listing the details of what has been updated. Unsuccessfully changed deployments are specified first in the file.

This file is an XML version of the PDF file created by the Publish Template Changes Wizard if using the SiteScope user interface to update deployed groups. For details on the report, see "Publish Template Changes Summary Report" on page 1049.

Deployment Results

When you copy the XML file, for both deploying and updating, into the persistency folder of the target SiteScope, the file is copied into one of two directories as follows:

- **<SiteScope root directory>\persistency\autodeployment\successHistory** directory includes those XML files that deployed or updated successfully all instances of the deployed group.
- **<SiteScope root directory>\persistency\autodeployment\failHistory** directory includes those XML files that failed to deploy or update any instance of the deployed group. If even one instance failed and all the others succeeded, the XML is published to this folder.

The XML file name is changed to include an underscore and a timestamp added to the original name of the XML file. For example the XML file named CPUgroups.XML that succeeded in deploying all its groups and instances is saved to the **<SiteScope root directory>\persistency\autodeployment\successHistory** directory and is now named CPUgroups_1203951216931.xml.

Tasks

How to Deploy a Monitoring Structure Using an XML File

This task describes how to perform an auto template deployment. You can follow the same steps for deploying a Solution Template.

This task includes the following steps:

- "Prerequisites" on page 1064
- "Create the XML file" on page 1065
- "Edit the XML file" on page 1065
- "Specify login details (mandatory if working in a secure environment)" on page 1066
- "Encrypt fields such as passwords - optional" on page 1066
- "Validate the XML file" on page 1067
- "Copy the validated XML to the SiteScope server machines" on page 1067
- "Check if deployment was successful" on page 1067

1 Prerequisites

Each SiteScope into which you want to automatically deploy a template must include the template within a template container. The template must have a group object at the top level. All other objects must be created within that group. The template can contain subgroups, monitors, alerts, one remote server, and variables.

If you are working with multiple SiteScopes:

- You can create the template in one SiteScope and export it to other SiteScopes using the Export/Import options in the Template containers context menu. For task details, see "Export Template Dialog Box" on page 1008 and "Import Template Dialog Box" on page 1010.

➤ If you are working in BSM, you can copy templates from one SiteScope to another using the Sync SiteScope Wizard in SAM Admin. For user interface details, see "Sync SiteScopes Wizard" in *Using System Availability Management* in the HP Business Service Management Documentation Library.

2 Create the XML file

You can create the XML file using one of these options:

➤ Right-click the template container and select **Generate XML** in the context menu. When deploying solution templates, this option appears at the template level. For user interface details, see "Generate Auto Deployment XML User Interface" on page 1075.

➤ Create the XML file using a dedicated XML application. The file must be a valid XML file and based on the XSD files located in the following directories:

➤ **<SiteScope root directory>/conf/xsds/deploy.xsd**

➤ **<SiteScope root directory>/conf/xsds/sitescope.xsd**

3 Edit the XML file

You must edit the XML file to enter the values necessary for deployment. For details on editing the file and a sample of the file, see "XML File Example and Variables" on page 1055.

For details on the XML file's tags, see "XML Tag Reference" on page 1071.

Note: If the XML is generated from the user interface, mandatory variable fields are generated based on the templates mandatory variables. If you create the XML file, and there are fields that are mandatory for successful deployment, you must make sure that these fields have been assigned values before deploying the XML.

---

4 Specify login details (mandatory if working in a secure environment)

If you are working in a secure environment, you must give a valid user name and password for each deployment. Login credentials can also be used in the **audit.log** file to track the identity of users making template changes.

To enable support for login in the API, add the following line (after </deploy:fullPathToDestinationGroup>):

```
<deploy:login user="<myUserName>" password="<myPassword>" />
```

Use the encryption tool and follow the steps in the procedure for encrypting the user name and password. For task details, see "How to Encrypt Text" on page 1068.

Note: XML files generated in earlier versions of SiteScope are supported, provided that you add the login when working in a secure environment.

---

5 Encrypt fields such as passwords - optional

For deploying templates that include fields that you do not want to appear in viewable text, use the encryption tool and follow the steps in the procedure for encrypting text. For task details, see "How to Encrypt Text" on page 1068.

6 Validate the XML file

We recommend validating the XML file before it is deployed. If the XML file does not pass validation when attempting to deploy, the deployment fails.

Use the validation tools located in the following directories:

- For Windows: **<SiteScope root directory>/tools/AutoDeployment/validate_template_xml.bat**
- For UNIX: **<SiteScope root directory>/tools/AutoDeployment/validate_template_xml.sh**

For concept details, see "XML Validator" on page 1060.

7 Copy the validated XML to the SiteScope server machines

Copy the XML file into the **\persistency\autodeployment** directory on each SiteScope machine where you want to deploy the templates in the XML.

The templates are automatically deployed every two minutes by default. You can change the frequency in Infrastructure Preferences in the following field: **Auto Deployment Check Frequency** (Property name: **_autoDeploymentCheckFrequency**).

8 Check if deployment was successful

You can check if the deployment was successful by searching in the target SiteScope's **<SiteScope root directory>\persistency\autodeployment** directory to see if the XML was copied into the **\successHistory** subdirectory or the **\failHistory** subdirectory.

For concept details, see "Deployment Results" on page 1063.

You can also check the SiteScope's Error Log.

How to Encrypt Text

This task describes how to encrypt text for a field that should not appear in viewable text, for example a password. This tool encrypts the field only in the XML; the templates themselves control the encryption of variables in the persistency directory.

To encrypt text for use in the deployment XML:

1 Run the following batch file:

- For Windows: <**SiteScope root directory**>**/tools/AutoDeployment/encrypt_password.bat**
- For UNIX: <**SiteScope root directory**>**/tools/AutoDeployment/encrypt_password.sh**

2 Open a command prompt window.

- In Windows, drag and drop the file into your command prompt window.
- In UNIX, you must run the .sh file from its directory.

3 Enter space and the password value (for example Mypassword). Click ENTER.

4 Use the returned string as a value for the encrypted variable in the XML file. You much change the value of the attribute **encrypted** to **yes** and the **value** of the variable attribute to the returned string.

For example, the following value was generated by the encryption tool:
<deploy:variables encrypted="yes" name="password" value="(sisp)d5JLOSWaVfE="/>

How to Update a Deployment

This task describes how to use the auto template deployment XML to update an existing, deployed group. You can update the structure of the deployment if the template was changed or update object properties by giving new values to the variables that are declared in the template for those properties.

The task follows the same steps as the task to deploy a template with the exceptions and additional information listed in the steps here. For details on the deployment task, see "How to Deploy a Monitoring Structure Using an XML File" on page 1064.

This task includes the following steps:

1 Prerequisites

The **Source Template** field of the deployed groups that you want to update must be identical to the template in the XML deployment update file. This is in addition to the updated template existing in the target SiteScope.

2 Create and edit the XML file to update objects and values

When working with the XML file, you must do the following:

- Use the **<templateDeploymentUpdate>** tag instead of the **<templateDeployment>** tag.
- Enter a **yes** or **no** value for the **enableDeleteOnUpdate** attribute of th**<templateDeploymentUpdate>** tag.
- Define the **deploy:fullPathToDestinationGroup** tag with the group name to be updated as the value for this tag.

For details on these tags and the update XML file, see "Update Deployment XML Tag Details" on page 1062.

3 Copy the publish template update XML to the target SiteScopes

Copy the publish template update XML to the target SiteScope's **persistency** directory as you would when deploying the auto template deployment XML file.

4 Encrypt text such as a password - optional

For task details, see "How to Encrypt Text" on page 1068.

5 Validate the publish template update XML

Use the validator tool to validate the edited XML file as you would when deploying the auto template deployment XML file.

6 Results report

After deploying the update auto template deployment XML, a results report file is created in XML format. These reports are available in the following location: **<SiteScope root directory>\persistency\autodeployment\reports**.

For user interface details, see "Template Update Report" on page 1062.

Reference

XML Tag Reference

The following tables list all the elements and attributes used in the auto template deployment XML files:

- "Elements Table" on page 1071
- "Attributes Table" on page 1073

Elements Table

Elements	Description
sitescope:sitescopeRoot	This must be the first tag in the XML file giving the instruction to create the deployment, the version of XML used, and the location of the XSD file. **Note**: This is the first element in all XML files related to SiteScope.
sitescope:template Deployment	This tag enables the deployment of the template or solution template, creating new group structures in the target SiteScope. This is the default tag used in the XML file when generated from the user interface.

Elements	Description
sitescope:template DeploymentUpdate	This tag enables publishing the changes of a template that has been updated. These changes can be applied to the monitoring structure of a group whose **Source Template** field matches the template identified in the XML. The XML file also enables you to update the values of the variables used in the template. For example, if you want to add alerts or an additional monitor to an existing group that was created by a template, you can modify the template and deploy it using this tag.
deploy:fullPathToTemplate	This tag gives the full path, within the SiteScope tree, of the template or solution template to be deployed. **Syntax:** <template container name>/<template name>
deploy:fullPathTo DestinationGroup	This tag gives the full path location within the SiteScope tree of the group name where the deployed monitoring structure is to be created. If this tag has no value, the deployment is created at the SiteScope node level.
deploy:mandatoryFields	The values within this tag are those variables that were selected as mandatory fields when the template was created. If there are any values appearing within this tag, they must be given a value in the <**deploy:globalVariables**> tag for global variables or the <**deploy:variables**> tag for other variables. If there are no corresponding values for these mandatory fields, the XML fails validation.
deploy:globalVariables	This tag marks the section of the file that includes the variables that are deployed across the entire selected template. Includes attributes. For details, see "Attributes Table" on page 1073.

Elements	Description
deploy:templateInstance DeployVariable	This tag marks the section of the file that includes the variables that are deployed per instance of the selected template. If the same variable appears in the **<deploy:globalVariables>**, the instance variable value overrides the global variable value only for the instance in which it appears. All other instances have the value entered in the **<deploy:globalVariables>** section. Includes attributes. For details, see "Attributes Table" on page 1073.
deploy:variables	This tag defines the variables and their values. Includes attributes. For details, see "Attributes Table" on page 1073.

Attributes Table

Parent Element	Attribute	Description
templateDeploymentUpdate	enableDeleteOnUpdate	Indicates whether any instances of objects appearing in a deployment of a template should be deleted when not appearing in the XML file used for updating the structure of a deployment. **Possible values**: yes, no For details on this option, see "Enable delete on update" on page 1042.

Parent Element	Attribute	Description
deploy:globalVariables deploy:templateInstanceDeployVariable	description	(Optional) User description for the deployment.
	connectToServer	(Optional) Verifies the monitor configuration properties in the template against the remote server on which the template is being deployed. This is the default behavior (even if this attribute is not specified). To avoid connecting to the remote server, add connectToServer="no" to the **<deploy:globalVariables>** or **<deploy:templateInstanceDeployVariable>** tag. **Possible values**: yes, no For details on this option, see "Verify monitor properties with remote server" on page 1026.
	accessControlled	(Optional) Tests the connection created from the template remote server after the template has been deployed. **Possible values**: true, false
deploy:variables	encrypted	Indicates whether the value of the variable's field is encrypted or not. **Possible values**: yes, no To encrypt a value, use the encryption tool to provide the value for the variable. For details, see "How to Encrypt Text" on page 1068.
	name	The name of the variable.
	value	The value of the variable.

Generate Auto Deployment XML User Interface

This dialog box enables you to create an XML file to use for automatically deploying the templates in the highlighted template container. After you generate the XML file, you can edit the file and use it to deploy the templates from the file directory not in the SiteScope user interface.

To access	Select the **Templates** context. In the template tree, right-click the template container for which you want to create an auto deploy XML file, and select **Generate XML**.
Relevant tasks	"How to Deploy a Monitoring Structure Using an XML File" on page 1064
See also	➤ "Auto Template Deployment Overview" on page 1054 ➤ "Template Tree" on page 95

User interface elements are described below:

UI Element	Description
File Name	Name of the XML file to create. This is the file you can edit and use to automatically deploy the templates in this template container.

UI Element	Description
Path	Location in which the XML file is saved. Accept the default location, or enter a different location. If the path is empty, the XML file is saved to the root drive where SiteScope is installed. **Default value:** <SiteScope_install_path>\SiteScope\persistency\autodeployment\drafts **Note:** If an XML file has been generated previously using the same **File Name** and **Path**, the previously saved XML file is not overwritten. The previous file is renamed with the following addition: **_bck<number of backup>**. For example, if you enter CPUtemplate as the **File Name** and accept the default location, the existing file in the default folder becomes CPUtemplate.xml_bck1 and the current XML file being generated is saved as CPUtemplate.xml.
Template Tree	Templates for which to create the XML file. The XML file's contents are based on the objects in the template you select. For each template selected, the generated XML includes a separate deploy section.

Troubleshooting and Limitations

This section describes troubleshooting and limitations when working with auto template deployment.

Note: All notes, limitations, and troubleshooting issues that apply to SiteScope templates, solution templates, and the Publish Template Changes Wizard also apply to the functionality of the auto template deployment.

This section includes:

I18N Users

- Do not edit the XML file using Notepad. The file cannot be parsed because Notepad adds an extra character to the beginning of the file. This character is not visible but prevents the file from being parsed when not in English. Use Wordpad or an XML editor instead.
- If the path to the SiteScope root directory includes non-English characters, the validation tool cannot be used to validate the XML before it is copied to the SiteScope's persistency directory. This means that there is no validation that the XML follows the XSD or that mandatory fields have values.

Solution Templates

You cannot perform auto template deployment for the following Solution Templates because the variables in these solution templates are dynamically created and cannot be given a value in the XML file:

- JBoss Application Server 4.x
- WebLogic Application Server
- WebSphere 5.x Application Server
- WebSphere 6.x Application Server

Characters Not Permitted in XML

Avoid using the ampersand (&), quote marks (“), and angle brackets (< >) characters, as they are not permitted in XML attribute values.

To escape illegal XML characters, use a common encoding, (for example, & instead of &), or enclose the character with the CDATA (character data) section. For details, see http://xmmssc-www.star.le.ac.uk/SAS/xmmsas_20070308_1802/doc/param/node24.html.

Unable to Auto Deploy Template with No Groups

If you attempt to automatically deploy a template where the template has no parent group defined (that is to say, the template has monitors directly under the root template), the deployment fails and the following error is written to the <**SiteScope root directory****logs**\>**error.log** file:

[Autodeployment new XML detection] (XMLAutomationParser.java:294) ERROR - Prerequisites of template structure are unmet. Template must be rooted by only one group.

Note that Auto deployment fails even if **Allow creation of template monitors directly under template** is selected in **Preferences** > **Infrastructure Preferences** > **Template Settings**.

Workaround: Deploy the template manually (right-click the template in the Template tree, and then select **Deploy Template**).

Updating Deployed Groups Using Auto Template Deployment XML

For limitations on using the auto template deployment XML to update an existing deployment, see "Notes and Limitations" on page 1033.

Part IX

Solution Templates

43

SiteScope Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Solution Templates Overview

SiteScope solution templates are preconfigured monitor set templates designed to monitor popular enterprise applications and network systems. Using solution templates, you can rapidly deploy a combination of standard SiteScope monitor types and solution-specific monitors with settings that are optimized for monitoring the availability, performance, and health of the target application or system. For example, the solutions for Microsoft Exchange monitoring include performance counter, event log, and Exchange application specific monitor types.

Deploying the solution creates a new monitor group container in which the individual solution monitors are added. You can deploy a solution template for each server in your environment. For solution templates that use the system variable SERVER_LIST, you can deploy the solution on multiple remote hosts.

This section also includes:

- "List of Solution Templates" on page 1085
- "Customizing Solution Templates" on page 1087
- "Notes and Limitations" on page 1087

List of Solution Templates

The following table lists solution templates available for SiteScope. For more information about each solution and the solution specific monitor types, see the chapter for the specific solution template.

Solution Name	Description
Failover Monitoring Solution Templates	Monitor the availability of primary and failover SiteScope machines when using SiteScope Failover Manager.
Active Directory Solution Templates	Monitors the performance and efficiency of Microsoft domain controllers (with or with global category) for Microsoft Windows 2000 and 2003, and Active Directory 2008 R2.
AIX Host Solution Template	Monitors performance, availability, and health for AIX host machines.
HP Quality Center Solution Templates	Monitors performance, availability, and health for HP Quality Center 9.x and 10.x application servers on Windows and UNIX, HP Quality Center license usage and expiration time on an Oracle Database server, and HP QuickTest Professional license server application and system availability.
HP Service Manager Solution Templates	Monitors HP Service Manager application servers availability and system status on Windows and UNIX platforms.
JBoss Application Server Solution Template	Monitors performance, availability, and health for JBoss environments.
Linux Host Solution Template	Monitors performance, availability, and health for Linux host machines.
Microsoft Exchange Solution Templates	Includes individual solution options for monitoring application health, message flow, and usage statistics for Microsoft Exchange 5.5, 2000, 2003, 2007, and 2010 servers.
Microsoft IIS Solution Templates	Monitors performance, availability, and health for IIS 6.0 and IIS 7.x environments.

Solution Name	Description
Microsoft Lync Server 2010 Solution Templates	Monitors performance, availability, and health for the following Microsoft Lync Server 2010 Servers: A/V Conferencing Server, Archiving Server, Director Server, Edge Server, Front End Server, Lync Server Event Log, Mediation Server, Monitoring Server, and Registrar Server.
Microsoft SharePoint 2010 Solution Templates	Monitors performance, availability, and health for Microsoft SharePoint 2010.
Microsoft SQL Server Solution Templates	Monitors performance, availability, and usage statistics for Microsoft SQL Server 2005 and 2008, and for Microsoft SQL Server 2008 R2.
Microsoft Windows Host Solution Template	Monitors performance, availability, and health for Microsoft Windows 2000, Windows XP, and Windows Server 2003 host machines.
.NET Solution Templates	Monitors performance, availability, and health of .NET applications and environments on Windows 2000, Windows XP, and Windows Server 2003.
Oracle Database Solution Template	Monitors performance, availability, and usage statistics for Oracle 9i and 10g databases.
SAP Solution Templates	Monitors performance, availability, and usage statistics for SAP system components.
Siebel Solution Templates	Monitors performance, availability, and usage statistics for Siebel Application Server installed on Windows and UNIX operating systems.
Solaris Host Solution Templates	Monitors performance, availability, and health for Solaris host machines.
VMware Host Solution Template	Monitors CPU, memory, storage, state, and network performance and usage statistics for the VMware Host server and on guest virtual machines on the host server.
WebLogic Solution Templates	Monitors performance, availability, and usage statistics for Oracle WebLogic application servers.
WebSphere Solution Templates	Monitors performance, availability, and usage statistics for IBM WebSphere Server 5.x application servers.

Customizing Solution Templates

Since a solution template is unlikely to match all your system configurations, you can customize the solution template to meet your system requirements as follows:

- Copy the solution template to a template container, modify it to suit your system requirements, and then deploy the modified solution template.
- Deploy the solution template, and modify it after the deployment to suit your system's requirements.

For example, when using the HP Quality Center Application Server solution template to monitor the repository disk variable, and the repository is on a different host to the application server, after deploying the template, you must change the repository disk utilization monitor to use the other host.

Notes and Limitations

- Errors detected during the creation of monitors using a solution template are independent of the status returned when the individual monitors are run. This means that the monitors may be created successfully but that the configuration settings may be incorrect or that the system being monitored is unavailable.
- After some solution templates are deployed, the relevant monitors may be defined with a BSM reporting level of **Disable reporting to BSM**. Therefore after deploying a solution template, we recommend that you check the monitors' reporting level. If you want to change the reporting level for the deployed monitors, you can use the Global Search and Replace wizard to update the reporting level option.
- Solution templates do not configure any automated alerts or reports for the monitors created. You may create and associate one or more alert definitions or reports to the monitors or monitor groups created by solution templates.

Tasks

How to Deploy a SiteScope Solution Template

This task describes the steps involved in deploying a solution template. Deploy a solution template for each server in your environment.

This task includes the following steps:

1 Prerequisites

- You must have the applicable SiteScope option license to use the Solution Template. Contact your HP sales representative for more information about Solution licensing.
- The license must be imported from a license file in **Preferences** > **General Preferences** > **Licenses**. For user interface details, see "General Preferences Page" on page 694.

2 Deploy the template

Select the method for deploying the solution template to a group:

- You can deploy a solution template directly from the user interface. In the template tree, right-click the solution template you want to deploy, and select **Deploy Template**. In the Select Group dialog box, select the monitor group into which you want to deploy the solution template. For user interface details, see "Select Group Dialog Box" on page 1022.

Note: Solutions that provide a number of templates (these are grouped in a template container), can be deployed to a group individually or simultaneously. For example, when deploying the Microsoft Exchange 2010 solution, you can select only the templates that you require, and deploy them against distributed Exchange server installations on separate servers. For details on deploying multiple templates simultaneously, see "Deploy multiple templates - optional" on page 1016.

- You can deploy a solution template using a CSV file that contains the variable values defined in the template. For concept details, see "Deploying a Template Using a CSV File" on page 1013. For task details, see "How to Deploy Template Using a CSV File" on page 1017.
- You can deploy and update the template using an XML file external to the SiteScope user interface. For concept details, see "Auto Template Deployment Overview" on page 1054. For task details, see "How to Deploy a Monitoring Structure Using an XML File" on page 1064.

3 Enter variable values for the template deployment

Complete the items on the Deployment Values page for the selected solution template. For user interface details, see the Deployment Values page for the specific solution template.

4 Configure alerts and reports

Configure alerts and reports for the newly created solution monitors.

For details on configuring alerts, see "How to Configure an Alert" on page 1443.

For details on configuring reports, see "How to Create a Report" on page 1508.

5 Results

The solution template creates a new monitor group container in which the individual solution monitors are added. The monitor group container is assigned a name in the format <Solution Template name> on <server_name> where server_name is the server selected from the **Server** box.

You can view, edit, and delete these monitors in the same way as any other monitors in SiteScope.

Note: If some of the monitors fail to deploy, a message is shown listing the names of the monitors together with a message describing the error.

Reference

Solution Templates Page

Displays the name and description of the selected solution template.

To access	Select the **Templates** context. In the template tree, expand the **Solution Templates** container and select the required template.
Important information	➤ Only licensed solution templates that are displayed with the  icon are configurable solution templates. ➤ The Search/Filter Tags pane is not available for filtering Solution Template objects.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	"Template Tree" on page 95

User interface elements are described below:

UI Element	Description
Name	Name of the solution template (read-only).
Description	Description of the solution template (read-only).

Troubleshooting and Limitations

This section describes troubleshooting and limitations for SiteScope solution templates.

➤ "Reinstalling the Solution Templates" on page 1092

➤ "Importing Templates" on page 1093

Reinstalling the Solution Templates

The installed solution templates are located in the **<SiteScope root directory>\persistency** directory. If the contents of this directory are deleted, the solution templates are not displayed in the template tree. To reinstall the solution templates, you must copy the solution template files back to the **persistency** directory.

Note: We do not recommend deleting the **persistency** directory as this permanently deletes all SiteScope configuration data and all historic data in BSM (if SiteScope is integrated with BSM).

To reinstall the solution template files:

1. Locate the solution template files in the following directory: **<SiteScope root directory>\export**.
2. Copy the contents of **<SiteScope root directory>\export** into **<SiteScope root directory>\persistency\import**.
3. Check that the solution templates have been reinstalled by locating them in the **Solution Templates** folder in the template tree.

Importing Templates

- When importing templates, if templates already exist with the same name in the same template container, the import may fail, due to unique name violation. To prevent this, rename the existing template containers.
- If the import fails or you no longer see the solution templates in the Solution Templates tree, you can restore the solution templates as described in "Reinstalling the Solution Templates" on page 1092. If the **\export** folder also contains the template examples, the template container should be renamed to prevent the unique name violations mentioned above.

44

Failover Monitoring Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Failover Monitoring Solution Templates Overview

SiteScope Failover Manager is a special version of SiteScope that includes automated failover functionality. It enables you to implement failover capability for infrastructure monitoring by making sure that a failed SiteScope machine is automatically and quickly replaced by a different machine, with little service disruption.

Failover Monitoring solution templates are preconfigured monitor set templates designed to monitor the failover environment. Using the Failover Monitoring solution templates, you can rapidly deploy solution-specific SiteScope monitors with settings that are optimized for monitoring the availability of primary and failover SiteScope machines.

When a primary SiteScope is registered to the Failover Manager configuration file, it is recommended to deploy the Failover Monitoring solution template (for Windows or UNIX) to the primary SiteScope, according to the platform on which SiteScope is running. A Failover Monitoring solution template should be deployed to each primary SiteScope server being monitored by the Failover Manager.

The solution template creates a monitor group container on the primary SiteScope in which the specially configured Failover monitors are added. The Failover monitors are SiteScope log monitors with settings that are optimized for monitoring the availability of the target primary SiteScope and the failover service.

After the solution template is deployed, you can configure alerts on the deployed monitors to notify you of changes in status on the primary SiteScope and when a failover occurs. For example, you can configure a Failover alert to receive email notification when the primary SiteScope goes down.

Note: For details on using SiteScope Failover Manager, see the *HP SiteScope Failover Manager Guide* PDF located in **<SiteScope root directory>\sisdocs\pdfs\SiteScopeFailover.pdf**.

Failover Template Monitors

The Failover Monitoring solution templates are located in the **Solution Templates** folder in the SiteScope template tree. All the monitors are Log File monitors which are configured to search for a particular text match in the Failover Manager **ha.log** file. The information from this file is used as a trigger for activating alert actions.

The monitoring frequency is defined by the **Frequency** setting in the Monitor Run Settings pane on the Failover monitor. By default, each monitor is set to run every 60 seconds.

The following table provides an overview of the monitors in the Failover Monitoring solution template.

Failover Monitors	Description	Threshold Settings
Failed to Start SiteScope Failover	This is a log monitor that is used to detect if the failover service has failed to start after the primary SiteScope has gone down. When the monitor is in error, the Failover Manager logs a message to the **ha.log** file, and the monitor checks for a match. Configure an alert to notify you if the monitor is in error.	Error if matches =="n/a'" or > 0 Good if ==0
Failed to Stop SiteScope Failover	This is a log monitor that is used to detect if the failover service has failed to stop after the Failover Manager has requested it to shutdown. When the monitor is in error, the Failover Manager logs a message to the **ha.log** file, and the monitor checks for a match. Configure an alert to notify you if the monitor is in error.	Error if matches =="n/a'" or > 0 Good if ==0
Primary SiteScope has Recovered	This is a log monitor that is used to detect if the primary SiteScope has recovered after a failure. The monitor is configured to be in error when there is match.	Error if matches =="n/a'" or > 0 Good if ==0

Failover Monitors	Description	Threshold Settings
Primary SiteScope is Down	This is a log monitor that is used to detect if a primary SiteScope has gone down. The monitor is in error status when the primary SiteScope is down.	Error if matches =="n/a'" or > 0 Good if ==0
Primary SiteScope Status Unknown	This is a log monitor that is used to detect if the primary SiteScope status is unknown. The Failover should not be up and running as a backup when the primary SiteScope status is unknown. The monitor is configured to be in error when there is match.	Error if matches =="n/a'" or > 0 Good if ==0

Tasks

How to Deploy a Failover Monitoring Solution Template

This task describes the steps involved in deploying a Failover Monitoring solution template.

This task includes the following steps:

- "Deploy the Failover Monitoring solution template" on page 1100
- "Modify Failover monitor configuration properties - optional" on page 1101
- "Configure alerts and reports" on page 1101
- "View monitor results during failover" on page 1101
- "View monitor results when the primary SiteScope recovers" on page 1101

1 Deploy the Failover Monitoring solution template

Deploy the Failover Monitoring solution template using one of the following methods:

- From the template tree in the user interface. For task details, see "How to Deploy Templates Using the User Interface" on page 1014.
- Using a CSV file. For task details, see "How to Deploy Template Using a CSV File" on page 1017.
- Using an XML file external to the SiteScope user interface. For task details, see "How to Deploy a Monitoring Structure Using an XML File" on page 1064.

Once deployed, the Failover Monitoring solution template creates a new monitor group container in which the individual Failover monitors are added. The monitor group container is assigned a name in the format Failover Monitors on <primary SiteScope installation path>.

For details on Failover Monitoring solution template properties, see "Failover Monitoring Solution Template Page" on page 1102.

2 Modify Failover monitor configuration properties - optional

You can modify monitor configuration properties for Failover monitors in the same way as any other monitors in SiteScope.

For example, you can modify conditions that determine the reported status of each monitor instance in the Threshold Settings. For details on modifying monitor thresholds, see "Threshold Settings" on page 457.

3 Configure alerts and reports

Configure alerts on the deployed Failover monitors to notify you of changes in status on the primary SiteScope and when a failover occurs. For details on configuring alerts, see "How to Configure an Alert" on page 1443.

You can also configure reports for the newly created Failover monitors. For details on configuring reports, see "How to Create a Report" on page 1508.

4 View monitor results during failover

If a primary SiteScope goes down, an alert is triggered notifying you of the change in status of the primary SiteScope. To view monitoring results during a failover, you need to redirect your Web browser to the address of the failover SiteScope server using the format:

http://<Failover Manager name>:<Failover Manager port>/SiteScope

For example, http://localhost:8080/SiteScope.

5 View monitor results when the primary SiteScope recovers

When the primary SiteScope recovers, an alert is triggered if an alert was configured on the **Primary SiteScope has Recovered** monitor. To view monitoring results, redirect your Web browser to the address of the primary SiteScope instance using the format:

http://<Primary SiteScope name>:<Primary SiteScope port>/SiteScope

Reference

Failover Monitoring Solution Template Page

This page enables you to deploy the Failover Monitoring solution template on the primary SiteScope server.

To access	Select the **Templates** context. In the template tree, expand the **Solution Templates** container and select the required Failover Monitoring template.
Relevant tasks	"How to Deploy a Failover Monitoring Solution Template" on page 1100
See also	"Failover Monitoring Solution Templates Overview" on page 1096

Failover Monitoring Solution Template for Windows

The Main Settings include the following elements:

UI Element	Description
Failover Manager host	The name of the Failover Manager host.
Failover Manager user name	The user name with administrator credentials that SiteScope should use to connect to the Failover Manager.
Failover Manager password	Password for the user name that SiteScope should use to connect to the Failover Manager.
Failover Manager ha.log path	The full UNC path to the Failover Manager **ha.log** file. **Default value:** \\<Failover Manager server>\SiteScope\logs\ha.log

UI Element	Description
Primary SiteScope installation path	The full installation path of the primary SiteScope server. **Default value:** \\\\<Shared folder>\\<Primary server>\\SiteScope **Syntax exceptions:** If meta characters are used in the installation path, they should be escaped if you want the characters to have their normal meaning. Meta characters can be escaped by preceding them with a backslash ("\").)
Log file encoding	If the log file content to be monitored uses an encoding that is different than the encoding used on the server where SiteScope is running, enter the encoding to use. This may be necessary if the code page which SiteScope is using does not support the character sets used in the target log file. This enables SiteScope to match and display the encoded log file content correctly. **Default value:** UTF-8
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

Failover Monitoring Solution Template for UNIX

The Main Settings include the following elements:

UI Element	Description
Failover Manager Host	The name of the Failover Manager host.
Failover Manager User	The user name with administrator credentials that SiteScope should use to connect to the Failover Manager.
Failover Manager Password	Password for the user name that SiteScope should use to connect to the Failover Manager.
Failover Manager HA Log	The full path to the Failover Manager **ha.log** file. **Default value:** /opt/HP/SiteScope/logs/ha.log
Primary SiteScope Installation Path	The full installation path of the primary SiteScope server. **Syntax exceptions:** If meta characters are used in the installation path, they should be escaped where you want the characters to have their normal meaning. Meta characters can be escaped by preceding them with a backslash ("\").) **Default value:** //<HA mounts>//<Primary server>//SiteScope
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

45

Active Directory Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Active Directory Solution Overview

You can use the Active Directory solution templates to provide monitoring of domain controller performance—services on which Active Directory depends—and distributed Active Directory performance.

The Active Directory solution templates deploy a set of monitors against a particular Domain Controller. These monitors encompass best practices monitoring for Active Directory. This template includes NT Event Log, Service, LDAP, performance counter and Active Directory Replication monitors.

The Active Directory solution templates provide comprehensive monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

The Active Directory solution templates support Microsoft Windows Server 2000, 2003, and 2008 R2.

Note:

- You must have the applicable SiteScope option license to use the Active Directory solution templates. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the Active Directory Solution is available in the SiteScope Active Directory Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_Active_Directory_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Active Directory Solution license key from HP.

Solution Template Monitors

The Active Directory solution templates deploy monitors that target the following aspects of Active Directory performance:

- **Domain controller performance.** This category refers to the low level health of each domain controller in the environment. The Active Directory solution template automatically configures monitors for domain controller health.
- **Dependent services.** Active Directory depends on several key services. Without these services, Active Directory can become unresponsive or fail altogether. The Active Directory solution template automatically configures monitors for a list of important services on which Active Directory performance is dependent.
- **Distributed Active Directory performance.** Perhaps the most important aspect and key indicator of Active Directory performance is how fast Active Directory is replicating changes out to all domain controllers. The Active Directory solution template automatically configures monitors for monitoring and testing replication of changes and updates.

Note: Some of the monitor types deployed by the solution templates can only be added to SiteScope by using the Active Directory Solution sets. For more information, see the section for the particular monitor types.

Tasks

How to Deploy the Active Directory Solution Templates

This task describes the steps involved in entering variables for the Active Directory solution template.

This task includes the following steps:

- "Deploy the solution template" on page 1109
- "Enter deployment values for the solution template" on page 1109

1 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

2 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Active Directory solution template. For user interface details, see "Active Directory Solution Template Page" on page 1110.

Reference

Active Directory Solution Template Page

This page enables you to deploy the SiteScope Active Directory solution templates.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required Active Directory solution template.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Active Directory Solution Templates" on page 1105 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
ReplicatingDomain Controllers	Comma separated list of domain controllers that replicate data from the domain controller selected above.
LDAPSecurity Principal	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.
LogicalDrive	Logical drive that this Domain Controller is using for its database and log files.
PASSWORD	Password for the user selected above.
HostName	Host part of the domain controller's host name (do not include the fully qualified domain name).

UI Element	Description
Global Catalog (AD with Global Catalog only)	Select if the Domain Controller is a Global Catalog server.
SERVER_LIST	Domain Controller that you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected
Test remote servers (AD 2008 R2 only)	Tests the connection created from the template remote server after the templates have been deployed. The test is performed in the background, enabling you to continue to use SiteScope. **Default value:** Not selected

46

AIX Host Solution Template

This chapter includes:

Concepts

Tasks

Reference

Concepts

AIX Host Solution Overview

The AIX Host solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the AIX host. The template supports the versions of AIX that are supported by SiteScope. For details, see "System Requirements" in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can create a Server-Centric report which displays data from three different metrics about the server being monitored.

Tip: We recommend using solution templates when creating the UNIX Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric report, see "Generating a Server-Centric Report" on page 1324.

The AIX Host solution template provides comprehensive AIX operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the AIX Host solution template. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the AIX Host Solutions settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs \SiteScope_OS_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

Solution Template Monitors

The AIX Host solution template deploys monitors that target the following aspects of AIX performance and health:

- CPU status and utilization details
- Memory status and utilization details
- File system status and utilization details

Tasks

How to Deploy the AIX Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the AIX Host solution template.

Note: The AIX Host solution template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Server-Centric Report support.

This task includes the following steps:

- "Prerequisites" on page 1116
- "Deploy the solution template" on page 1117
- "Enter deployment values for the solution template" on page 1117

1 Prerequisites

- The SiteScope server must be able to connect to the target AIX host.
- The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test (**Remote Servers** > **UNIX Remote Servers**). For details, see "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

Note:

- 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.

---

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the AIX solution template. For user interface details, see "AIX Host Solution Template Page" on page 1118.

Reference

AIX Host Solution Template Page

This page enables you to deploy the SiteScope AIX solution template.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select **AIX Host**.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "AIX Host Solution Template" on page 1113 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
SERVER_LIST	Name of the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a UNIX connection profile, see "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <**SiteScope root directory**>**logs****silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

47

HP Quality Center Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

HP Quality Center Solution Templates Overview

The HP Quality Center solution templates are templates that you can use to deploy a collection of monitors configured with default metrics that test the availability of HP Quality Center 9.x and 10.x application servers, license status on HP Quality Center 9.2 and 10.0 database servers, and HP QuickTest Professional license server application and system availability.

The HP Quality Center solution templates provide comprehensive HP Quality Center monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy performance monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the HP Quality Center solution templates. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the HP Quality Center solution is available in the SiteScope Quality Center Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_HP_QC_Best_Practices.pdf**. This is a password protected document. The password is provided along with the HP Quality Center Solution license key from HP.

This section also includes:

- "Solution Template Monitors" on page 1123
- "Monitoring Quality Center Third Party Applications" on page 1123

Solution Template Monitors

The HP Quality Center solution includes solution templates for monitoring the following key components:

- **HP Quality Center Application Server for UNIX/Windows.** Use this solution template to monitor the availability and performance of the HP Quality Center application server on the operating system on which the application is installed.
- **HP Quality Center 9.2/10.0 License Status.** Use this solution template to monitor HP Quality Center license usage and expiration time on an HP Quality Center database server (the solution template has been certified on an Oracle and Microsoft SQL database).
- **HP QuickTest Professional License Server.** Use this solution template to monitor the availability and performance of the HP QuickTest Professional License Server.

Monitoring Quality Center Third Party Applications

We recommend using other SiteScope solution templates, monitors, or both, to monitor Quality Center third party components, such as the application server on which Quality Center is deployed, and the database it uses.

For details on the solutions that are recommended for monitoring Quality Center third party components, see the tables below:

Database Server Monitoring

Database Type	Recommended Solution
Oracle	"Oracle Database Solution Template" on page 1223
Microsoft SQL Server	"Microsoft SQL Server Solution Templates" on page 1197
LDAP	"LDAP Monitor" on page 239

Application/Web Server Monitoring

Application/Web Server Type	Recommended Solution
Apache Server	"Apache Server Monitor" on page 39
JBoss	"JBoss Application Server Solution Template" on page 1149
Microsoft IIS	"Microsoft IIS Solution Templates" on page 1175 "Microsoft IIS Server Monitor" on page 333
WebLogic 6.x-8.x, 9.x-10.x	"WebLogic Solution Templates" on page 1267
WebSphere 5.x, 6.x	"WebSphere Solution Templates" on page 1277
Other Web/Application Servers that support JMX access (JSR 160)	"JMX Monitor" on page 227

Tasks

How to Deploy the HP Quality Center Solution Template

This task describes the steps involved in entering variables and deploying the HP Quality Center solution templates.

This task includes the following steps:

- "Prerequisites" on page 1125
- "Deploy the solution template" on page 1127
- "Enter deployment values for the solution template" on page 1127

1 Prerequisites

HP Quality Center Application Server for Windows:

- The SiteScope server must have access to the Quality Center components.
- You should have the following information:
  - Quality Center application version (9.2, 10.0)
  - Full host name and login credentials for the application server
  - Quality Center repository disk or repository location if it is located on another host
  - Port used in the login URL (usually none, which means that port 80 is used)

Note: This solution template is not supported on SiteScopes installed on UNIX platforms.

HP Quality Center Application Server for UNIX:

- The SiteScope server must have access to the Quality Center components.
- You should have the following information:
  - Quality Center application version (9.2, 10.0)
  - UNIX operating system type
  - Full host name and login credentials for the Application server
  - System file system
  - Quality Center repository disk or repository location if it is located on another host
  - Port used in the login URL (usually none, which means that port 80 is used)
  - Name of the java process command that runs the Quality Center application on the UNIX operating system. (you can use "ps -ef | grep java")

HP Quality Center 9.2/10.0 License Status:

- The SiteScope server must have access to the Quality Center 9.2 or 10.0 components.
- You should have the following information on the Quality Center database:
  - Database host name
  - Type (Oracle, Microsoft SQL, MSDE 2000)
  - Driver (possibly a SiteScope built-in database driver)
  - Database Connection URL
  - Database user name and password

HP QuickTest Professional License Server:

- The SiteScope server must have access to the QuickTest Professional License server.
- You should have the QuickTest Professional License server host name and login credentials.

Note: This solution template is not supported on SiteScopes installed on UNIX platforms.

---

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the HP Quality Center solution template. For user interface details, see "HP Quality Center Solution Template Page" on page 1128.

Reference

HP Quality Center Solution Template Page

This page enables you to deploy the HP Quality Center solution templates for monitoring the HP Quality Center 9.x and 10.x application servers on Windows and UNIX platforms, and license usage and expiration time on an HP Quality Center 9.2 or 10.0 database server. The templates also enable you to monitor HP QuickTest Professional license server application and system availability.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required HP Quality Center solution template.
Important information	The solution template uses the Ping monitor to monitor system availability. If Ping traffic is blocked on your network, you should use Port monitor instead.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "HP Quality Center Solution Templates Overview" on page 1122 ➤ "Troubleshooting and Limitations" on page 1138 ➤ "Template Tree" on page 95

HP Quality Center Application Server for Windows

The Main Settings include the following elements:

UI Element	Description
Application server host name	Host name of the Quality Center application server.
Application server user name	Login user name for the host on the Quality Center application server.
Application server password	Password for the host on the Quality Center application server.
System disk	Logical disk drive where the Quality Center application server is installed. **Default value:** C
Repository disk	Logical disk drive where the Quality Center repository is located. If the repository is located on another host, enter the system disk drive and alter the Repository Disk Utilization monitor after you deploy your template. **Default value:** D
Site Administration path	Suffix for the Quality Center Site Administration URL. **Default value:** qcbin/SiteAdmin.htm. For Quality Center version 9.x, change this to sabin.
Application port	Port used in the login URLs to the Quality Center application. Usually no port is specified which means port 80 is used. **Default value:** 80
Maximum round trip time (milliseconds)	Value in milliseconds, used as an error status threshold for a reasonable round trip time for getting a response from you application URLs. **Default value:** 1500 milliseconds
Quality Center service name	Name of the Quality Server service. **Default value:** HP Quality Center. For Quality Center version 9.x, change this to Mercury Quality Center.

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\ silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected
Test remote servers (HP Quality Center Application Server for Windows/UNIX only)	Tests the connection created from the template remote server after the template has been deployed. The test is performed in the background, enabling you to continue to use SiteScope. **Default value:** Not selected

HP Quality Center Application Server for UNIX

The Main Settings include the following elements:

UI Element	Description
Application server host name	Host name for the Quality Center application server.
Application server user name	Login user name for the host on the Quality Center application server.
Application server password	Password for the host on the Quality Center application server.

UI Element	Description
UNIX operating system	UNIX operating system type, such as Solaris, Red Hat Enterprise Linux. The complete list of UNIX operating system types is available in the **Operating system** field of the New/Edit UNIX Remote Server dialog box. **Default value:** Linux
System file system	File system where the Quality Center application is installed.
Repository file system	File system where the Quality Center repository is located. If the repository is located on another host, enter the system disk file system, and alter the Repository Disk Utilization monitor after you deploy your template.
Site Administration path	Suffix for the Quality Center Site Administration URL. **Default value:** qcbin/SiteAdmin.htm. For Quality Center version 9.x, change this to sabin.
Application port	Port used in the login URLs to the Quality Center application. Usually no port is specified which means port 80 is used. **Default value:** 80
Maximum round trip time (milliseconds)	Value in milliseconds, used as an error status threshold for a reasonable round trip time for getting a response from you application URLs. **Default value:** 1500 milliseconds

UI Element	Description
Quality Center process unique name	Name used to identify the Quality Center java process from the other processes running on the system. It can be the Quality Center process name, or a unique part of it taken from the java process command that runs the Quality Center application on the UNIX operating system (you can use ps -ef | grep java).
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\ silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

HP Quality Center 9.2/10.0 License Status

The Main Settings include the following elements:

UI Element	Description
Site Administration database host	Host name where the Quality Center Site Administration is installed.
Database driver	Database driver used for connecting to your database. If a custom driver is used, the driver must also be installed in the **<SiteScope root directory>\WEB-INF\lib directory**. **Default value:** com.inet.ora.OraDriver (supports Oracle Database). For Microsoft SQL, use com.mercury.jdbc.sqlserver.SQLServerDriver.
Connection URL (full)	Quality Center database connection URL. **Examples:** jdbc:inetora:[host]:[port]:[sid] (for Oracle Database) jdbc:mercury:sqlserver://labm1qcrnd05.devlab.ad:1433;DatabaseName=May22_2008_db (for Microsoft SQL)
Connection URL (part 0-3)	If your connection URL is composed of semicolon (;) separated values, enter each part in a separate field in addition to the full **Connection URL (full)** field. **Example:** Connection URL (part 0) = jdbc:mercury:sqlserver://labm1qcrnd05.devlab.ad:1433 Connection URL (part 1) = DatabaseName=May22_2008_db Otherwise enter your whole connection URL in Connection URL (part 0) for example: Connection URL (part 0) = jdbc:inetora:[host]:[port]:[sid] **Note:** The reason for this separation is that the connection URL is used as a Script monitor parameter, and the semicolon (;) character is not permitted for security reasons.

UI Element	Description
Database user	User name required for querying the database. The specified user name must have privileges to run the SELECT queries on the ADMIN and SESSION_LICENSE tables of the Site Administration database.
Database password	Password required for the given user name to log on to the database and run the SELECT queries.
Database password - encrypted	Encrypted form of the database password. To get the encrypted password, run the following tool on your password: **<SiteScope root directory>\tools\AutoDeployment\ encrypt_password.bat <password>** For UNIX platforms, run **enrypt_password.sh <password>**. **Note:** The encrypted password is used as a Script monitor parameter, and is required for security reasons.
Admin table name	Name of the Quality Center ADMIN table. **Default value:** ADMIN (supports Oracle database). For Microsoft SQL database, use td.ADMIN.
Session license table name	Name of the Quality Center Session License table. **Default value:** SESSION_LICENSE (supports Oracle database). For Microsoft SQL database, use td.SESSION_LICENSE.
SiteScope expiration error status (days remaining)	License expiration error threshold. Each License Expiration Status deployed monitor is in error status if the number of days until the license expires is less than the number specified here. **Default value:** 7 days
SiteScope expiration warning status (days remaining)	License expiration warning threshold. Each License Expiration Status deployed monitor is in warning status if the number of days until the license expires is less than the number specified here. **Default value:** 30 days

UI Element	Description
Number of free licenses for error	License usage error threshold. Each License Usage Status deployed monitor is in error status if the number of free licenses is less than the number specified here. **Default value:** 5
Number of free licenses for warning	License usage warning threshold. Each License Usage Status deployed monitor is in warning status if the number of free licenses is less than the number specified here. **Default value:** 20
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\ silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

Note:

- The Quality Center license is in XML format that is stored in the ADMIN table on the Site Administration database. It contains information about the Quality Center license expiration and quota for each of the different Quality Center modules (for example, Defects, Requirements, and so forth). The XML format is different for Quality Center 9.2 and Quality Center 10.0. Another table named SESSION_LICENSE contains an entry on real time for each logged in session and the license type used.
- To calculate the license usage and expiration, the SiteScope solution template uses a Script monitor that runs a script (**runQCLicenseTool.bat** on Microsoft Windows platforms, and **runQCLicenseTool.sh** on UNIX platforms). The script queries the Quality Center database, and returns the following information for the requested license type to the Script monitor:
  Total=<total quota>;used=<currently used of this type>;free=<total-free>;exp_days=<left days for license to expire>.

HP QuickTest Professional License Server

The Main Settings include the following elements:

UI Element	Description
QTP license server host name	Host name for the QuickTest Professional license server.
QTP license server user name	User name for the QuickTest Professional license server system login.
QTP license server password	Password for the QuickTest Professional license server system login.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\ silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

Troubleshooting and Limitations

If you encounter monitors that have a **content match error** after deploying the solution template, it is possible that your Quality Center does not support this type of license.

- If this is the case, you should delete the unsupported monitor.
- If the monitor is supported, you should check the log file: **<SiteScope root directory>\scripts\qc_license_tool.log**.

  To set the log file to debug, open **<SiteScope root directory>\conf\ems\tools\conf\core\Tools\log4j\PlainJava\log4j.properties**

  and set

  loglevel=DEBUG

48

HP Service Manager Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

HP Service Manager Solution Overview

SiteScope's HP Service Manager solution templates enable you to monitor and troubleshoot HP Service Manager application servers availability and system status on Windows and UNIX platforms. They measures HP Service Manager load balancer status, shared memory usage, and monitors logs for fatal errors. They can also be used to monitor HP Service Manager in Horizontal Scaled mode. The templates supports Service Manager 7.11.

The HP Service Manager solution templates provide comprehensive monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduces the time to configure and deploy performance monitors, and helps identify both real-time performance bottlenecks and longer term trends.

Note:

- You must have the applicable SiteScope option license to use the HP Service Manager solution templates. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the Service Manager solution templates is available in the Service Manager Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_HP_SM_Best_Practices.pdf**. This is a password protected document. The password is provided along with the HP Service Manager Solution license key from HP.

Solution Template Monitors

The HP Service Manager solution templates create a dynamic set of monitors that target the HP Service Manager server performance and health on Windows and UNIX platforms. For details on the monitors, see the SiteScope HP Service Manager Server Best Practices document.

Tasks

How to Deploy the HP Service Manager Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the HP Service Manager solution template.

This task includes the following steps:

1 Prerequisites

- The HP Service Manager solution templates supports Service Manager 7.11 only.
- All processes to be monitored must be up and running when deploying the template. If SiteScope does not find the processes when it tries to create the target monitor, a "No counters selected" error is displayed and the monitor is not created.

  Workaround: If not all processes are up and running, you can copy the template to your own template container and delete the processes monitors. You can later create them manually, or deploy another copy of the template that contains only the processes monitors.

➤ For the HP Service Manager for Windows solution template, the **sm-lbstatus-win-ssh.bat** and **sm-shm-win-ssh.bat** scripts must be run on the Microsoft Windows remote server where HP Service Manager is installed. For details, see step 2 below.

Note: The HP Service Manager for UNIX solution template uses the **sm-shm.txt** and **sm-lbstatus.txt** files located in **<SiteScope root directory>/scripts.remote** to run commands on the remote Service Manager UNIX host.

---

2 Run the sm-lbstatus-win-ssh.bat and sm-shm-win-ssh.bat scripts (for HP Service Manager for Windows)

a Install and configure the SSH Server (OpenSSH). For details, see "How to Configure Remote Windows Servers for SSH monitoring" on page 647.

b On the machine where SiteScope is installed, find the file called **RemoteNTSSH.zip** in the **<SiteScope root directory>\tools** directory. Unzip the **RemoteNTSSH.zip** file on the remote monitored Service Manager host. Place the contents of the zip file into the **C:\Documents and Settings\Administrator** folder.

c On the machine where SiteScope is installed, find the file called **SM_Scripts_win_ssh.zip** in the **<SiteScope root directory>\tools\ServiceManager** directory. Unzip the file on the remote monitored Service Manager host to **C:\Documents and Settings\Administrator\scripts** (The zip contains the **sm-lbstatus-win-ssh.bat** and **sm-shm-win-ssh.bat** files.) Make sure both scripts have execute permissions. If you are running Service Manager in Horizontally Scaled mode, you need to repeat this on every system.

d Share the Service Manager logs folder. Right-click the **logs** folder and select **Properties** > **Sharing**. Select **Share this folder**, and enter a **Share name**. Set the share permissions for the user that SiteScope monitor uses to run the monitors on that machine, and click **OK**.

3 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

4 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the HP Service Manager solution template. For user interface details, see "HP Service Manager Solution Template Page" on page 1145.

Reference

HP Service Manager Solution Template Page

This page enables you to deploy the HP Service Manager solution template.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required HP Service Manager solution template.
Important information	➤ If you are running HP Service Manager in Horizontally Scaled mode, you need to deploy and configure the HP Service Manager solution template on every system. ➤ All processes to be monitored must be up and running when deploying the template. If you get a "no counters selected" error, it means that some processes are down. To resolve this problem, make a copy of the template and delete the monitors for which you get errors before deploying the template. ➤ The solution template uses the Ping monitor to monitor system availability. If Ping traffic is blocked on your network, you should use the Port monitor, and use Global Search and Replace to replace the dependency from the Ping monitor to the Port monitor.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "HP Service Manager Solution Templates" on page 1139 ➤ "Template Tree" on page 95

HP Service Manager for Windows

The Main Settings include the following elements:

UI Element	Description
SM installation partition	Disk drive where HP Service Manager is installed. **Default value:** C
Application server host name	Name of the application server host.
User name	Login name to access the application server using this profile.
Password	Application server login password for this user.
Installation path	Path to the directory on which HP Service Manager binary is running. **Default value:** C:\Program Files\HP\Service Manager 7.11\Server\RUN
CPU error threshold	Threshold for triggering CPU errors. **Default value:** 90
CPU warning threshold	Threshold for triggering CPU warnings. **Default value:** 80
Memory error threshold	Threshold for triggering memory errors. **Default value:** 2202012 KB
Memory warning threshold	Threshold for triggering memory warnings. **Default value:** 1782580 KB
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected

UI Element	Description
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected
Test remote servers	Tests the connection created from the template remote server after the template has been deployed. The test is performed in the background, enabling you to continue to use SiteScope. **Default value:** Not selected

HP Service Manager for UNIX

The Main Settings include the following elements:

UI Element	Description
SM installation partition	Disk drive where HP Service Manager is installed.
Application server host name	Name of the application server host.
User name	Login name to access the application server using this profile.
Password	Application server login password for this user.
UNIX operating system	UNIX operating system on which HP Service Manager is running.
UNIX connection method	Method used to connect to the UNIX operating system.
Shell prompt	Prompt output when the remote system is ready to handle a command (for Telnet or Rlogin connection method only).
Installation path	Path to the directory on which HP Service Manager binary is running.

UI Element	Description
CPU error threshold	Threshold for triggering CPU errors. **Default value:** 90
CPU warning threshold	Threshold for triggering CPU warnings. **Default value:** 80
Memory error threshold	Threshold for triggering memory errors. **Default value:** 2202012 KB
Memory warning threshold	Threshold for triggering memory warnings. **Default value:** 1782580 KB
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected
Test remote servers	Tests the connection created from the template remote server after the template has been deployed. The test is performed in the background, enabling you to continue to use SiteScope. **Default value:** Not selected

49

JBoss Application Server Solution Template

This chapter includes:

Concepts

Tasks

Reference

Concepts

JBoss Application Server Solution Overview

The JBoss Application Server solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of JBoss application servers. The template supports JBoss Application Server versions 4.0.x and 4.2.x.

The JBoss Application Server solution template provides comprehensive JBoss monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the JBoss Application Server solution template. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the JBoss solution is available in the SiteScope JBoss Application Server Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_JBoss_Best_Practices.pdf**. This is a password protected document. The password is provided along with the JBoss Application Server solution license key from HP.

Solution Template Monitors

The JBoss Application Server solution template creates a dynamic set of monitors that target the JBoss application server performance and health. The exact monitor set depends on the entities you select during the solution template deployment. For details on the monitors, see the SiteScope JBoss Application Server Best Practices document.

Tasks

How to Deploy the JBoss Application Server Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the JBoss Application Server solution template.

This task includes the following steps:

1 Prerequisites

- The JBoss solution template supports JBoss application servers 4.0.x and 4.2.x only.
- You must know the URL for gathering JMX statistics (including the host name and port of the JMX instance), and the JMX user name and password.
- SiteScope and the target server can run on the same host.
- You must start JBoss in a particular way, so that SiteScope can monitor it. For details, see step 2 below.

2 Start JBoss

To enable SiteScope to monitor JBoss, you should specify the following options for the JBoss JVM:

```
-Dcom.sun.management.jmxremote.port=12345 (any other port can be used of
course; then it must be specified during ST deployment)
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false
-Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServer
BuilderImpl
-Djboss.platform.mbeanserver
-Dcom.sun.management.jmxremote
```

You can perform this using the following batch file:

```
@echo off
set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.port=12345
set JAVA_OPTS=%JAVA_OPTS% -
Dcom.sun.management.jmxremote.authenticate=false
set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.ssl=false
set JAVA_OPTS=%JAVA_OPTS% -
Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServer
BuilderImpl
set JAVA_OPTS=%JAVA_OPTS% -Djboss.platform.mbeanserver
set JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote
call run.bat -b my-jboss-host
```

Note:

- **run.bat** is the default script used to start JBoss.
- **-b** option binds JBoss 4.2.2 to the correct network interface (it binds only to localhost by default making it inaccessible from other hosts).
- You can build a similar script for UNIX.

---

3 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

4 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the JBoss Application Server solution template. For user interface details, see "JBoss Solution Template Page" on page 1155.

Reference

JBoss Solution Template Page

This page enables you to deploy the JBoss Application Server solution template.

Description	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select **JBoss AS 4.x**.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "JBoss Application Server Solution Template" on page 1149 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
JMX_URL	URL to gather JMX statistics. Typically the URL is in the format: service:jmx:rmi:///jndi/rmi://{hostname}:{port}/jmxrmi. Enter the host name and port of the JMX instance you want to monitor.
USERNAME	User name for connection to the JMX application (optional).
Password	Password for connection to the JMX application (optional).
Counters	Displays the server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.

UI Element	Description
Get Counters	Opens the Get Counters dialog box, enabling you to select the entities you want to monitor. For each instance, a specific set of monitors and thresholds is created. For details, see the SiteScope JBoss Application Server Best Practices Guide which can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_JBoss_Best_Practices.pdf**.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

50

Linux Host Solution Template

This chapter includes:

Concepts

Tasks

Reference

Concepts

Linux Host Solution Overview

The Linux Host solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the target Linux host. The template supports the versions of Linux that are supported by SiteScope. For details, see "System Requirements" in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can create a Server-Centric report which displays data from three different metrics about the server being monitored.

Tip: We recommend using solution templates when creating the UNIX Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric report, see "Generating a Server-Centric Report" on page 1324.

The Linux Host solution template provides comprehensive Linux operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the Linux Host solution template. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the Linux Host Solutions settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_OS_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

Solution Template Monitors

The Linux Host solution template deploys monitors that target the following aspects of Linux performance and health:

- CPU status and utilization details
- Memory status and utilization details
- File system status and utilization details

Tasks

How to Deploy the Linux Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Linux Host solution template.

Note: The Linux Host solution template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Server-Centric Report support.

This task includes the following steps:

- "Prerequisites" on page 1160
- "Deploy the solution template" on page 1161
- "Enter deployment values for the solution template" on page 1161

1 Prerequisites

- The SiteScope server must be able to connect to the target Linux host.
- The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test (**Remote Servers** > **UNIX Remote Servers**). For details, see "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

Note:

- 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.

---

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Linux Host solution template. For user interface details, see "Linux Host Solution Template Page" on page 1162.

Reference

Linux Host Solution Template Page

This page enables you to deploy the Linux Host solution template.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select **Linux Host**.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Linux Host Solution Template" on page 1157 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
SERVER_LIST	Name of the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a UNIX connection profile, see "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <**SiteScope root directory**>**logs****silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

51

Microsoft Exchange Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Microsoft Exchange Solution Overview

The Microsoft Exchange solution templates provide monitoring of performance, availability, and usage statistics for:

- Microsoft Exchange 5.5 Server
- Microsoft Exchange 2000 Server
- Microsoft Exchange 2003 Server
- Microsoft Exchange 2007 Server (version 8.0)
- Microsoft Exchange 2010 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.

The Microsoft Exchange solution templates provide comprehensive Microsoft Exchange system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the Microsoft Exchange solution templates. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the Microsoft Exchange Solution is available in the SiteScope Microsoft Exchange Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_Exchange_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Microsoft Exchange Solution license key from HP.

Solution Template Monitors

The Microsoft Exchange solution templates deploy monitors that target the following aspects of Microsoft Exchange performance and health:

- **Basic server/OS performance.** This category refers to the system-level health of a server. The Microsoft Exchange solution templates automatically configure monitors for server health.
- **Application performance.** Application performance is a measure of how well specific Exchange components are functioning. The Microsoft Exchange solution templates automatically configure monitors for a list of important Exchange application components.

- **Mail protocol response time.** Perhaps the most important aspect and key indicator of Microsoft Exchange performance is mail protocol response time. While Microsoft Exchange can use many protocols, the MAPI protocol is commonly used in Microsoft networks.
- **Usage statistics.** The last category related to Microsoft Exchange performance is usage. While usage in and of itself is not necessarily a key indicator of performance, changes in usage can affect overall Microsoft Exchange performance. In addition, Microsoft Exchange usage statistics help IT organizations spot trends and plan for the future. The Microsoft Exchange solution templates automatically configure monitors for a list of important Microsoft Exchange usage parameters.

Note: Some of the monitor types deployed by the solution templates can only be added to SiteScope by using the Microsoft Exchange solution templates. See the section for the particular monitor types for more information.

Tasks

How to Deploy Microsoft Exchange Solution Templates

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft Exchange solution template.

This task includes the following steps:

1 Prerequisites

Before deploying a Microsoft Exchange solution template, you must perform specific steps depending on the solution template you want to deploy.

- **Microsoft Exchange 5.5, 2000, 2003 solutions.** These solution templates make use of the SiteScope MAPI monitor. Successful deployment of this monitor type requires specific setup configuration relating to the mailbox owners and the SiteScope service. For the MAPI Monitor system requirements, see "MAPI Monitor Overview" in the *SiteScope Monitor Reference*.
- **Microsoft Exchange 2007, 2010 solutions.** These solution templates make use of the Microsoft Exchange 2007 and 2010 monitors. Successful deployment of these monitor types require specific setup configuration. For details, see "Microsoft Exchange 2007/2010 Monitor Overview" in the *SiteScope Monitor Reference*.

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

Note: The Microsoft Exchange 2010 solution provides a number of templates in a template container, that can be deployed either individually, or simultaneously, to a group. This enables you to select only the templates that you require, and to deploy them against distributed Exchange server installations on separate servers. For details on deploying multiple templates simultaneously, see "Deploy multiple templates - optional" on page 1016.

---

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Microsoft Exchange solution template. For user interface details, see "Microsoft Exchange Solution Template Page" on page 1171.

Reference

Microsoft Exchange Solution Template Page

This page enables you to deploy the Microsoft Exchange solution templates for monitoring Microsoft Exchange 5.5, 2000, 2003, 2007 (version 8.0), and 2010 servers.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required Microsoft Exchange solution template.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Microsoft Exchange Solution Templates" on page 1165 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
Domain (Exchange 2007 and 2010 only)	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.
Mailbox	Name (alias) of the mailbox to be used for testing email round trip times using MAPI. This is often the email account name but it may be a different name. **Tip:** We recommend copying the mailbox name as it appears in the E-Mail Account properties for the email account you are using for this solution.

UI Element	Description
MailUser (Microsoft Exchange 5.5, 2000, and 2003 only)	Windows account login name for the user for which email round trip times is tested using MAPI.
MailDomain (Microsoft Exchange 5.5, 2000, and 2003 only)	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.
MAILPASSWORD (Microsoft Exchange 5.5, 2000, and 2003 only)	Windows account login password for the user name entered above.
SERVER_LIST	Name of the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.
AuthenticationUser (Microsoft Exchange 2003 only)	User name to use when querying the server for mailbox and public folder statistics. The statistics are gathered by using WMI (Windows Management Instrumentation), so the user name entered here must have permissions to read WMI statistics on the server from WMI namespace root\MicrosoftExchangeV2. If this box is left blank, the user that SiteScope is running as is used.
AUTHENTICATION PASSWORD (Microsoft Exchange 2003 only)	Password for the user entered above for gathering WMI statistics, or leave this blank if the user box is left blank.

UI Element	Description
Exchange PS Console File Path (Microsoft Exchange 2007 and 2010 only)	Path to the Microsoft Exchange Management Shell PowerShell console file. **Default value:** C:\Program Files\Microsoft\Exchange Server\Bin\ExShell.psc1
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

52

Microsoft IIS Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Microsoft IIS Solution Overview

The Microsoft IIS solution templates are templates that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of Microsoft IIS 6 and IIS 7.x servers.

The Microsoft IIS solution templates provide comprehensive IIS monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the Microsoft IIS solution templates. Note that there is a different license for the IIS 6 and the IIS 7.x solution template. Contact your HP sales representative for more information about solution licensing.
- An in-depth description of the IIS solution templates is available in the SiteScope Microsoft IIS Best Practices document (**SiteScope_IIS_Best_Practices.pdf**). This document can be found in the **<SiteScope root directory>\sisdocs\pdfs** directory. This is a password protected document. The password is provided along with the IIS solution license key from HP.

IIS Solution Template Monitors

The Microsoft IIS solution templates deploy monitors that target the following services and aspects of IIS server performance and health:

- Active Server Pages (ASP errors, requests, templates, sessions, transactions)
- FTP service, Web service, SMTP server, NNTP server, HTTP/HTTPS services, MSMQ Queue service, IIS Server, Global IIS status, IIS WAS, IIS W3SVC, IIS Windows Log, Indexing services
- IIS statistics as a Windows process

Tasks

How to Deploy the Microsoft IIS Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft IIS solution template.

This task includes the following steps:

1 Prerequisites

- The SiteScope server must be able to connect to the target Microsoft IIS host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see "Microsoft Windows Resources Monitor Overview" in the *SiteScope Monitor Reference*.
- The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Remote Servers** > **Microsoft Windows Remote Servers**). For details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603.

  Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, see "Set Domain Privileges for SiteScope Monitoring" on page 591.

Note: SiteScope and the target IIS server can run on the same host.

---

2 Configure the server environment (for Microsoft IIS 6 only)

Configure the IIS Server so that it contains the ASP component path in the components tree.

a In the Control Panel, select **Add or Remove Programs** > **Add/Remove Windows Components**.

b In Windows Component Wizard, on the Windows Components page, highlight **Application Server**, and click **Details**.

c In Application Server, select the **ASP.NET** check box.

d Highlight **Internet Information Services (IIS)**, and then click **Details**.

e In Internet Information Services (IIS), select the **World Wide Web Service** check box, and then click **Details**.

f In World Wide Web Service, select the **Active Server Pages** check box, and then click **OK**.

g In Internet Information Services (IIS) click **OK**.

h In Application Server, ensure that the **Internet Information Services (IIS)** check box is selected, and then click **OK** to install the components.

i Click **Next**, and when the Windows Components Wizard completes, click **Finish**.

j To enable ASP.NET, select **Administrative Tools** > **Internet Information Services (IIS) Manager** in the Control Panel.

k In the console tree, expand the local computer, and then click **Web Service Extensions**.

l In the details pane, click **ASP.NET**, and then click **Allow**.

3 Configure the server environment (for Microsoft IIS 7.x only)

Configure the IIS Server so that it contains the ASP component path in the components tree.

a Start the Server Manager (click **Start**, click **Run**, and then type CompMgmtLauncher).

b In the tree view, select **Roles**, and in the **Roles** pane click **Add Roles**.

c In the Add Roles Wizard, click **Select Server Roles**, select the **Web Service (IIS)** check box, click **Next**, and then click **Next** again.

If the "Add features required for Web Server (IIS)?" message is displayed, click **Click Add Required Features**.

d In the Select Role Services window, make sure that the **ASP.NET and ASP** service is selected (under **Application Development**).

4 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

5 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Microsoft IIS solution template. For user interface details, see "Microsoft IIS Solution Template Page" on page 1181.

Reference

Microsoft IIS Solution Template Page

This page enables you to deploy the Microsoft IIS 6 solution template.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required Microsoft IIS solution template (**Microsoft IIS 6** or **Microsoft IIS 7.x**).
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Microsoft IIS Solution Templates" on page 1175 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
SERVER_LIST	Name of the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

53

Microsoft Lync Server 2010 Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Microsoft Lync Server 2010 Solution Overview

You can use the Microsoft Lync Server 2010 solution templates to provide monitoring of different aspects of the Microsoft Lync Server 2010 server. This includes:

- **Microsoft A/V Conferencing Server.** Monitors the server performance statistics of the Microsoft Lync A/V Conferencing Server. A/V conferencing enables real-time audio and video A/V communications between your users (provided they have appropriate client devices such as headsets for audio conferences and web cams for video conferences). A/V Conferencing Server provides A/V conferencing functionality to your deployment. It can be collocated with Front End Server, or deployed separately as a single server or A/V Conferencing Server pool.
- **Microsoft Archiving Server.** Monitors the server performance statistics of the Microsoft Lync Archiving Server. The Archiving Server enables you to archive instant messaging (IM) communications and meeting content for compliance reasons. Corporations and other organizations are subject to an increasing number of industry and government regulations that require the retention of specific types of communications. With the Archiving Server feature, Microsoft Lync Server 2010 communications software provides a way for you to archive IM content, conferencing (meeting) content, or both, that is sent through Lync Server 2010. If you deploy Archiving Server and associate it with Front End pools, you can set it to archive instant messages and conferences and specify the users for which archiving is enabled.

- **Microsoft Director Server.** Monitors the server performance statistics of the Microsoft Lync Director Server. A Director is a server running Microsoft Lync Server communications software that authenticates user requests, but does not home any user accounts or provide presence or conferencing services. Directors are most useful in deployments that enable external user access, where the Director can authenticate requests before sending them on to internal servers. Directors can also improve performance in organizations with multiple Front End pools.
- **Microsoft Edge Server.** Monitors the server performance statistics of the Microsoft Lync Edge Server. The Edge Server enables your users to communicate and collaborate with users outside the organization's firewalls. These external users can include the organization's own users who are currently working offsite, users from federated partner organizations, and outside users who have been invited to join conferences hosted on your Lync Server deployment. Edge Server also enables connectivity to public IM connectivity services, including Windows Live, AOL, and Yahoo!.
- **Microsoft Front End Server.** Monitors the server performance statistics of the Microsoft Lync Front End Server. The Front End Server is the core server role, and runs many basic Lync Server functions. The Front End Server, along with the Back End Servers, which provide the database, are the only server roles required to be in any Lync Server Enterprise Edition deployment.

  A Front End pool is a set of Front End Servers, configured identically, that work together to provide services for a common group of users. A pool provides scalability and failover capability your users.

  Front End Server includes the following functionality:

  - User authentication and registration
  - Presence information and contact card exchange
  - Address book services and distribution list expansion
  - IM functionality, including multiparty IM conferences
  - Web conferencing and application sharing (if deployed)

  - Application hosting services, for both applications included with Lync Server (for example, Conferencing Attendant and Response Group application) and third-party applications
  - Application services for application hosting and hosts applications (for example, Response Group application, and several others)

- **Microsoft Mediation Server.** Monitors the server performance statistics of the Microsoft Lync Mediation Server. The Mediation Server is a necessary component for implementing Enterprise Voice and dial-in conferencing. The Mediation Server translates signaling and, in some configurations, media between your internal Lync Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk. On the Lync Server side, Mediation Server listens on a single mutual TLS (MTLS) transport address. On the gateway side, Mediation Server listens on a single TCP and single TLS transport address or a single TLS transport address. All qualified gateways must support TLS, but can enable TCP as well.
- **Microsoft Monitoring and CDR Server.** Monitors the server performance statistics of the Microsoft Lync Monitoring and CDR Server. The Monitoring Server collects data about the quality of your network media, in both Enterprise Voice calls and A/V conferences. This information can help you provide the best possible media experience for your users. It also collects call error records (CERs), which you can use to troubleshoot failed calls. Additionally, it collects usage information in the form of call detail records (CDRs) about various Lync Server features, so that you can calculate return on investment of your deployment, and plan the future growth of your deployment.
- **Microsoft Registrar Server.** Monitors the server performance statistics of the Microsoft Lync Registrar Server. The Lync Server 2010 Registrar is a new server role that enables client registration and authentication and provides routing services. It resides along with other components on a Standard Edition Server, Enterprise Front End Server, Director, or Survivable Branch Appliance. A Registrar pool consists of Registrar Services running on the Lync Server pool and residing at the same site.

For Microsoft Lync Server 2010 monitors, you can create a Server-Centric report which displays data from three different metrics about the server being monitored.

The Microsoft Lync Server 2010 solution templates provide comprehensive monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the Microsoft Lync Server 2010 solution templates. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the Microsoft Lync Server 2010 Solution is available in the SiteScope Microsoft Lync Server 2010 Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_MS_Lync_Server_2010_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Microsoft Lync Server 2010 Solution license key from HP.

Tasks

How to Deploy the Microsoft Lync Server 2010 Solution Templates

This task describes the steps involved in entering variables for the Microsoft Lync Server 2010 solution template.

This task includes the following steps:

- "Deploy the solution template" on page 1188
- "Enter deployment values for the solution template" on page 1188

1 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

2 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Microsoft Lync Server 2010 solution template. For user interface details, see "Microsoft Lync Server 2010 Solution Template Page" on page 1189.

Note: The Microsoft Lync Server 2010 solution provides a number of templates in a template container, that can be deployed either individually, or simultaneously, to a group. This enables you to select only the templates that you require. For details on deploying multiple templates simultaneously, see "Deploy multiple templates - optional" on page 1016.

Reference

Microsoft Lync Server 2010 Solution Template Page

This page enables you to deploy the various Microsoft Lync Server 2010 solution templates (Microsoft Archiving Server, Microsoft A/V Conferencing Server, Microsoft Director Server, Microsoft Edge Server, Microsoft Front End Server, Microsoft Mediation Server, and Microsoft Monitoring and CDR Server, Microsoft Registrar Server). For template descriptions, see "Microsoft Lync Server 2010 Solution Overview" on page 1184.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates** > **Microsoft Lync Server 2010**, and select the required Microsoft Lync Server 2010 solution template.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Microsoft Lync Server 2010 Solution Templates" on page 1183 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
Host	The host name of the Microsoft Lync Server 2010 instance you want to monitor.
User	The user name with admin credentials on the Microsoft Lync Server 2010 instance.
Password	Password for the user on the Microsoft Lync Server 2010.

UI Element	Description
Connection method	The method used to connect to the server. Options are: NetBIOS, WMI, or SSH. **Default value:** NetBIOS
Remote server encoding	The encoding of the remote server. **Default value:** Cp1252
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected
Test remote servers	Tests the connection created from the template remote servers after the templates have been deployed. The test is performed in the background, enabling you to continue to use SiteScope. **Default value:** Not selected

54

Microsoft SharePoint 2010 Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Microsoft SharePoint 2010 Solution Overview

You can use the Microsoft SharePoint 2010 solution templates to provide monitoring of SharePoint environments—to understand how the SharePoint Server 2010 system is running, and to monitor important events, performance counters, and services, found in SharePoint 2010 products.

The Microsoft SharePoint 2010 solution templates deploy a set of monitors (Microsoft Windows Event Log, Microsoft Windows Resources, CPU, Disk Space, and SQL) that target services and aspects of the Microsoft SharePoint 2010 performance and health. These monitors encompass best practices monitoring for Microsoft SharePoint 2010.

The Microsoft SharePoint 2010 solution templates provide comprehensive monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the Microsoft SharePoint 2010 solution template. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the Microsoft SharePoint 2010 Solution is available in the SiteScope Microsoft SharePoint 2010 Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_SharePoint_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Microsoft SharePoint 2010 Solution license key from HP.
- The Microsoft SharePoint 2010 solution templates are also supported in SiteScopes that are running on UNIX versions if the remote server being monitored has been configured for SSH and the SSH connection method is used in the template. For details, see "SiteScope Monitoring Using Secure Shell (SSH)" in *Using SiteScope*.

Solution Template Monitors

The Microsoft SharePoint 2010 solution template deploys monitors that target availability, performance, and health of the following aspects of a SharePoint environment:

- IIS Process
- InfoPath Service
- Publishing Service
- Search Service
- Service Application
- SharePoint Server
- SQL Server

Tasks

How to Deploy the Microsoft SharePoint 2010 Solution Templates

This task describes the steps involved in deploying the Microsoft SharePoint 2010 solution templates.

This task includes the following steps:

- "Deploy the solution template" on page 1194
- "Enter deployment values for the solution template" on page 1194

1 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

2 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Microsoft SharePoint 2010 solution template. For user interface details, see "Microsoft SharePoint 2010 Solution Template Page" on page 1195.

Note: The Microsoft SharePoint 2010 solution provides a number of templates in a template container, that can be deployed either individually, or simultaneously, to a group. This enables you to select only the templates that you require. For details on deploying multiple templates simultaneously, see "Deploy multiple templates - optional" on page 1016.

Reference

Microsoft SharePoint 2010 Solution Template Page

This page enables you to deploy the SiteScope Microsoft SharePoint 2010 solution template.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates** > **Microsoft SharePoint 2010**, and select the required SharePoint template.
Important information	The Microsoft SharePoint 2010 solution templates are also supported in SiteScopes that are running on UNIX versions if the remote server being monitored has been configured for SSH and the SSH connection method is used in the template. For details, see "SiteScope Monitoring Using Secure Shell (SSH)" in *Using SiteScope*.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Microsoft SharePoint 2010 Solution Templates" on page 1191 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
Host	The host name of the Microsoft SharePoint instance.
User Name	The user name with admin credentials on the monitored Microsoft SharePoint instance.
Password	Password for the user on the monitored Microsoft SharePoint instance.

UI Element	Description
Connection method	The method used to connect to the server. Options are NetBIOS, WMI, and SSH. **Default value:** NetBIOS
Remote server encoding:	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 value:** Cp1252
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected
Test remote servers	Tests the connection created from the template remote servers after the template has been deployed. The test is performed in the background, enabling you to continue to use SiteScope. **Default value:** Not selected

55

Microsoft SQL Server Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Microsoft SQL Server Solution Overview

The Microsoft SQL Server solution template are templates that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of Microsoft SQL servers. The templates support Microsoft SQL Server 2005, 2008, and 2008 R2.

The Microsoft SQL Server solution templates provide comprehensive Microsoft SQL server monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the Microsoft SQL Server solution templates. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the Microsoft SQL Server solutions is available in the SiteScope Microsoft SQL Server Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_MSSQL_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Microsoft SQL Server solution license key from HP.

Solution Template Monitors

The Microsoft SQL Server solution templates deploy monitors that target the following aspects of Microsoft SQL server performance and health:

- CPU status and utilization details
- Memory status and utilization details
- Disk utilization information
- SQL Server availability
- SQL Server objects (Buffer Manager, Databases, Locks, Transactions, Batch request, Cache))
- SQL Server resources (space available, percentage of currently connected users, I/O utilization, latches, mirroring, replication, data access)
- Errors in SQL Server

The Microsoft SQL Server solution makes use of the SiteScope Database Counter monitor, Microsoft SQL Server monitor, and Microsoft Windows Resources monitor. For detailed information about these monitors, see "Database Counter Monitor Overview" on page 104, "Microsoft SQL Server Monitor Overview" on page 358, and "Microsoft Windows Resources Monitor Overview" on page 408.

Tasks

How to Deploy the Microsoft SQL Server Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft SQL Server solution template.

This task includes the following steps:

- "Prerequisites" on page 1200
- "Deploy the solution template" on page 1201
- "Enter deployment values for the solution template" on page 1201

1 Prerequisites

- The SiteScope server must be able to connect to the target Microsoft SQL host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see "Microsoft Windows Resources Monitor Overview" in the *SiteScope Monitor Reference*.
- The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Remote Servers** > **Microsoft Windows Remote Servers**). For details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603.

  Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, see "Set Domain Privileges for SiteScope Monitoring" on page 591.

➤ The SQL Server user must have **VIEW SERVER STATE** permissions on the monitored SQL Server instance to retrieve data from SQL Server System Views. For more information about granting permissions on Microsoft SQL Server, see http://msdn2.microsoft.com/en-us/library/ms186717.aspx.

Note: SiteScope and the target Microsoft SQL Server can run on the same host.

---

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Microsoft SQL Server solution template. For user interface details, see "Microsoft SQL Server Solution Template Page" on page 1202.

Reference

Microsoft SQL Server Solution Template Page

This page enables you to deploy the Microsoft SQL Server solution template for monitoring key components on a Microsoft SQL Server.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required solution (**Microsoft SQL Server** or **Microsoft SQL Server 2008 R2**).
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Microsoft SQL Server Solution Templates" on page 1197 ➤ "Template Tree" on page 95

Microsoft SQL Server (for Microsoft SQL Server 2005 and 2008)

User interface elements are described below:

UI Element	Description
Login to Microsoft SQL Server	Login name for the user on the monitored Microsoft SQL Server instance.
Microsoft SQL Server password	Password for the user on the monitored Microsoft SQL Server instance.
Microsoft SQL Server URL	URL for the monitored Microsoft SQL Server instance. ➤ Replace ${host} with the host name on which the Microsoft SQL Server is running. This must be the same as the host name defined for the Windows remote machine. For details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603. ➤ Replace ${port} with the port number on which the Microsoft SQL Server accepts connections. By default, the port is 1433. **Example:** jdbc:mercury:sqlserver://doors:1433

UI Element	Description
SERVER_LIST	Name of the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

Microsoft SQL Server 2008 R2

User interface elements are described below:

UI Element	Description
Microsoft SQL Server URL	URL for the monitored Microsoft SQL Server instance. ➤ Replace ${host} with the host name on which the Microsoft SQL Server is running. This must be the same as the host name defined for the Windows remote machine. For details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603. ➤ Replace ${port} with the port number on which the Microsoft SQL Server accepts connections. By default, the port is 1433. **Example:** jdbc:mercury:sqlserver://doors:1433
Login to Microsoft SQL Server 2008 R2	Login name for the user on the monitored Microsoft SQL Server 2008 R2 instance.
Password to Microsoft SQL Server 2008 R2	Password for the user on the monitored Microsoft SQL Server 2008 R2 instance.
Microsoft SQL Server 2008 R2 agent service name	Name of the SQL Server 2008 R2 agent service. **Default value:** SQL Server (MSSQLSERVER)
Microsoft SQL Server 2008 R2 service instance name	Name of the SQL Server 2008 R2 service instance. **Default value:** SQL Server (MSSQLSERVER)
Microsoft SQL Server 2008 R2 service name	Name of the SQL Server 2008 R2 service. **Default value:** SQL Server

UI Element	Description
SERVER_LIST	Name of the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

56

Microsoft Windows Host Solution Template

This chapter includes:

Concepts

Tasks

Reference

Concepts

Microsoft Windows Host Solution Overview

The Microsoft Windows Host solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the Windows host. The template supports Microsoft Windows 2000, Windows XP, Windows Server 2003, and Windows Server 2008.

For Microsoft Windows Resource monitors, you can create a Server-Centric report which displays data from three different metrics about the server being monitored.

Tip: We recommend using solution templates when creating the Microsoft Windows Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric report, see "Generating a Server-Centric Report" on page 1324.

The Microsoft Windows Host solution template provides comprehensive Windows operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the Microsoft Windows Host solution template. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the Microsoft Windows Host Solution settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_OS_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

Solution Template Monitors

The Microsoft Windows Host solution template deploys monitors that target the following aspects of Microsoft Windows performance and health:

- High-level CPU status and utilization details
- High-level Memory status and utilization details
- Disk utilization information

Tasks

How to Deploy the Microsoft Windows Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Microsoft Windows Host solution template.

Note: The Microsoft Windows Host Solution deploys a Microsoft Windows Resource Monitor for each target host. This monitor is an additional monitor that is required for Server-Centric Report support.

This task includes the following steps:

- "Prerequisites" on page 1211
- "Deploy the solution template" on page 1211
- "Enter deployment values for the solution template" on page 1211

1 Prerequisites

- The SiteScope server must be able to connect to the target Windows host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see "Microsoft Windows Resources Monitor Overview" in the *SiteScope Monitor Reference*.
- The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Remote Servers** > **Microsoft Windows Remote Servers**). For details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603.

  Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, see "Set Domain Privileges for SiteScope Monitoring" on page 591.
- SiteScope and the target server can run on the same host if SiteScope is installed on a Windows operating system supported by the template. The template supports Microsoft Windows 2000, Windows XP, Windows Server 2003, and Windows Server 2008.

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Microsoft Windows Host solution template. For user interface details, see "Microsoft Windows Host Solution Template Page" on page 1212.

Reference

Microsoft Windows Host Solution Template Page

This page enables you to deploy the Microsoft Windows Host solution template for monitoring a Microsoft Windows 2000, Windows XP, and Windows Server 2003 operating system.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select **Microsoft Windows Host**.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Microsoft Windows Host Solution Template" on page 1207 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
SERVER_LIST	Name of the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a Windows connection profile, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

57

.NET Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

.NET Solution Overview

The .NET solution templates enable you to monitor .NET applications of servers that run a Windows operating system. This solution template deploys a set of monitors that test the health, availability, and performance of a .NET application and .NET environment on the Windows host. The templates support Windows 2000, Windows XP, and Windows Server 2003.

The .NET solution templates provide comprehensive .NET monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the .NET solution templates. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the .NET Solution is available in the SiteScope .NET Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_NET_Best_Practices.pdf**. This is a password protected document. The password is provided along with the .NET Solution license key from HP.

Solution Template Monitors

The .NET solution templates deploy monitors that target the following aspects of .NET performance and health:

- **.NET CLR Data.** This category refers to the common language runtime data (environment of .NET applications). It is designed to check several resource statistics for the .NET CLR for selected application. The .NET solution template automatically configures monitors for server health.
- **ASP.NET.** This category is designed to check several resource statistics for the ASP.NET. It gathers common information about application restarts and whole ASP.NET system stability. The .NET solution template automatically configures monitors for server health.
- **ASP.NET Applications.** This category is designed to check several resource statistics for the selected ASP.NET application. It gathers common information about application cache, errors, and other critical information. The .NET solution template automatically configures monitors for server health.

Tasks

How to Deploy the .NET Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the .NET solution template.

This task includes the following steps:

1 Prerequisites

- SiteScope server must be able to connect to the target Windows host. Use the Microsoft Windows Resources Monitor to monitor the server performance statistics from remote Windows servers. The Microsoft Windows Resource monitor may require special configuration. For details, see "Microsoft Windows Resources Monitor Overview" in the *SiteScope Monitor Reference*.
- The target server must be added to SiteScope as a Windows remote machine and should pass the Windows remote test (**Remote Servers** > **Microsoft Windows Remote Servers**). For details, see "New/Edit Microsoft Windows Remote Server Dialog Box" on page 603.

  Alternatively, you can set domain privileges to permit SiteScope to access remote servers. For details, see "Set Domain Privileges for SiteScope Monitoring" on page 591.
- SiteScope and the target .NET application can run on the same host if SiteScope is installed on a Windows operating system supported by the template. The template supports Windows 2000, Windows XP, and Windows Server 2003.

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the .NET solution template. For user interface details, see ".NET Solution Template Page" on page 1220.

Reference

.NET Solution Template Page

This page enables you to deploy the .Net solution template for monitoring .NET application and .NET environments.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required .NET solution template.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ ".NET Solution Templates" on page 1215 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
Server	Name of the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. See "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586 for the steps you use to create a Windows connection profile.
ASP.NET Application (ASP.NET Application only)	Name of the ASP.NET application you want to monitor. The name must be as it appears in the Task Manager.
Instance (.NET CLR Data only)	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).

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <**SiteScope root directory**>**logs****silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

58

Oracle Database Solution Template

This chapter includes:

Concepts

Tasks

Reference

Concepts

Oracle Database Solution Overview

You can use the Oracle Database solution templates to deploy a set of monitors that test the health, availability, and performance of an Oracle database. The deployed monitors check general system statistics, such as cache hit ratios and disk I/O, and include tools that provide diagnostic information about important aspects of the database. This solution can be used with Oracle 9i and 10g databases.

This solution uses the Database Counter Monitor to collect performance metrics from JDBC-accessible databases. In addition, you can use the Oracle Database solution template to deploy a collection of monitors configured with default metrics.

Important system metrics are computed with data retrieved from system tables in the Oracle database. A wide range of Oracle system tables such as V$SYSSTAT, V$LATCH, V$ROLL_STAT, and V$BUFFER_POOL_STATISTICS are consulted to produce these metrics. In this way, the Oracle Database Solution implements the equivalent of many of the system monitoring scripts that come bundled with the Oracle installation.

The Oracle Database solution templates provide comprehensive Oracle database monitoring without requiring the SiteScope user or the IT organization to be an expert on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the Oracle Database solution template. Contact your HP Sales representative for more information about Solution licensing.
- An in-depth description of the Oracle Database Solution is available in the SiteScope Oracle Database Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_Oracle_Database_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Oracle Database Solution license key from HP.

Solution Template Monitors

The Oracle Database solution template deploys monitors that target the following aspects of Oracle performance and health:

- **General System Statistics.** The most important V$SYSSTAT statistics are monitored by default in the monitors deployed by the Oracle Database Solution. Where applicable, these metrics are combined to calculate deltas and rates on a per-second or per-transaction basis. When monitoring the important metrics from the V$ tables in the database, the Oracle Database Solution is a replacement for manually generated SQL scripts.
- **Oracle Logs.** Important Oracle log files are monitored for ORA- errors. Users may customize these monitors to look for specific text in a log file, depending on their database configuration.
- **Diagnosing Database Problems.** In addition to the deployed monitors, Oracle Solution offers several tools that can be used to gain diagnostic information about a database. Resource-intensive SQL statements, shared server process contention, and the number of sessions waiting for specific events are all examples of the diagnostic data that these tools can provide.

Tasks

How to Deploy Oracle Database Solution Templates

This task describes the steps involved in configuring the server environment and entering variables for the Oracle Database solution template.

This task includes the following steps:

- "Prerequisites" on page 1226
- "Deploy the solution template" on page 1226
- "Enter deployment values for the solution template" on page 1226

1 Prerequisites

- You must have CREATE SESSION system privileges to successfully deploy the Oracle Database solution template.
- Before deploying the Oracle Database solution template, consult the documentation for the Database Counter Monitor and the Log File Monitor (see "Database Counter Monitor Overview" and "Log File Monitor Settings" in the *SiteScope Monitor Reference*) for information about some of the prerequisites and parameters required by the solution template. For example, you find more information on installing the Oracle JDBC driver needed to communicate with the database and the format of the log file path parameter.

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Oracle Database solution template. For user interface details, see "Oracle Database Solution Template Page" on page 1230.

Reference

Oracle Database Solution Template Tools

The Oracle Database solution template deploys several tools that you can use to gather diagnostic information about an Oracle database. These tools are deployed to the same group as the monitors that are deployed by the solution template. They are displayed in much the same way as monitors but they are set as disabled. These tools are identified by the bold text **Solution Tool** in the **Status** field of the group content table. Although the Solution tools are listed in the monitor table, they are not monitor instances. They do not run automatically, do not display a status based on action results, nor do they trigger alerts. They are preconfigured actions that make use of a SiteScope Diagnostic Tool to check certain statistics from the Oracle database that may indicate a performance problem.

When the user clicks on one of these Solution Tools, SiteScope makes a custom SQL query to the database by using the Database Connection Test tool. The results of the query are found in a table at the bottom of the page. From this page, the tool may be run as many times as necessary by clicking the Connect and Execute Query button. Bear in mind that some tools may incur substantial overhead on the database, so executing them in quick succession is not recommended.

List of Oracle Database Solution Tools

The following describes tools deployed as part of the Oracle Database Solution:

Oracle Solution Tool Name	Description and Usage Guidelines
Top Ten SQL Statements in Logical IOs Per Row	This tool performs a query which is designed to locate the most resource-intensive SQL statements being run in the database. The V$SQL table is queried for the ten SQL statements which are performing the most logical IOs per row are displayed in a table. 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 affect on database resources and should not be run 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.

To run the Oracle Database Solution tools:

1. Click the group name for the group where the Oracle Solution monitors are deployed. The Group Detail page opens.
2. Find the Solution Tool for the action that you want to run. See the **Name** column for the Solution Tool for a description of the action performed by that tool.
3. Click the **Tools** link to the right of the tool **Name** to run the action. The Database Connection Test page opens. From this page, the tool may be run as many times as necessary by clicking the **Connect and Execute Query** button.

Note: We do not recommend running the tools in quick succession, since some Solution Tools may create significant overhead on the database depending on the query.

The upper portion of the Database Connection Test page displays the database connection parameters used for the test. The results of the tool query are found in a table near the bottom of the page. Review the results based on the Description and Usage Guidelines for that tool.

Oracle Database Solution Template Page

This page enables you to deploy the Oracle Database solution template.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select **Oracle Database 9i** and **10g**.
Important information	You must have CREATE SESSION system privileges to successfully deploy the Oracle Database 9i and 10g solution template.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Oracle Database Solution Template" on page 1223 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
DatabaseConnection URL	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=<sid>. **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.
DatabaseDriver	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**.

UI Element	Description
OracleAlertLogPath	Full path to the Oracle alert log. For Windows machines, this should be the full UNC path. Enter the full path to the Oracle alert log. Consult your database administrator or the Oracle documentation for information about how to access this file.
OracleListenerLog Path	Full path to the Oracle listener log. For Windows machines, this should be the full UNC path. Consult your database administrator or the Oracle documentation for information about how to access this file.
DatabaseUserName	User name that SiteScope should use to connect to the database.
DATABASEPASSWORD	Password for the user name that SiteScope should use to connect to the database.
Log 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.
SERVER_LIST	Name of the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a connection profile, see "How to Configure SiteScope to Monitor a Remote Microsoft Windows Server" on page 586 or "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

59

SAP Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

SAP Solution Overview

The SAP solution includes solution templates for the monitoring the following key SAP components:

- The SiteScope SAP R/3 Application Server solution template provides the tools you use to monitor the availability, usage statistics, and server performance statistics for SAP R/3 systems. This solution template deploys a set of monitors that test the health, availability, and performance of SAP R/3 servers.
- The SiteScope SAP NetWeaver Application Server solution enables you to monitor the availability and server statistics for SAP Java Web application server clusters. You can use this solution template to deploy monitors for server-wide resources and metrics.

The SAP solution templates deploy a collection of monitors configured with metrics to report on availability and performance. These monitoring configurations have been researched using best practice data and expertise from various sources.

The SAP solution templates provide comprehensive SAP monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note: You must have the applicable SiteScope option license to use the SAP R/3 Application Server and SAP NetWeaver Application Server solution templates. Contact your HP sales representative for more information about licensing for solution templates.

Tasks

How to Deploy the SAP Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the SAP solution template.

This task includes the following steps:

- "Prerequisites" on page 1235
- "Deploy the solution template" on page 1236
- "Enter deployment values for the solution template" on page 1236

1 Prerequisites

For SAP R/3 Application Server:

- SAP Java Connector libraries should be copied to the required SiteScope folders.
- You must know the user name and password that SiteScope must use to log into the SAP R/3 server.

  For more information on system and configuration requirements, see "SAP CCMS Monitor Overview" in the *SiteScope Monitor Reference*. This monitor is deployed as part of the SAP R/3 solution template.

For SAP NetWeaver Application Server:

- SAP Java Web application server libraries must be copied to the required SiteScope folders.
- You must know the user name and password that SiteScope must use to log into the SAP Java Web application server.

  For more information on system and configuration requirements, see "SAP Java Web Application Server Monitor Overview" in the *SiteScope Monitor Reference*. This monitor is deployed as part of the SAP NetWeaver Application Server solution template.

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the SAP solution template. For user interface details, see "SAP Solution Template Page" on page 1237.

Reference

SAP Solution Template Page

This page enables you to deploy the SAP solution templates for monitoring key components on SAP CCMS and SAP Java Web Application Servers.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required SAP solution template.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "SAP Solution Templates" on page 1233 ➤ "Template Tree" on page 95

SAP R/3 Application Server

The Main Settings include the following elements:

UI Element	Description
CLIENT_NUMBER	Client to use for connecting to SAP.
Password	Password required to connect to the SAP server.
USER_NAME	User name required to connect to the SAP server.
SYSTEM_NUMBER	System number for the SAP server.

UI Element	Description
APPLICATION_SERVER	Address of the SAP server you want to monitor.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

SAP NetWeaver Application Server

The Main Settings include the following elements:

UI Element	Description
TARGET_SERVER_NAME	Address of the SAP Java Web Application Server you want to monitor.
USER_NAME	User name required to connect to the SAP Java Web Application Server.
PORT	Port for the SAP Java Web Application Server.
Password	The password required to connect to the SAP Java Web Application Server.

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

60

Siebel Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Siebel Solution Overview

The SiteScope Siebel solution templates provide efficient and thorough monitoring of performance, availability, and usage statistics for Siebel Application, Gateway, and Web servers installed on Microsoft Windows and UNIX operating systems. There are separate solution templates for servers installed on UNIX and Windows platforms.

The primary solution template for Siebel is the Siebel Application Server template. You use this template to deploy monitoring for the core of the Siebel application. You use the Siebel Gateway Server and Siebel Web Server templates if these optional components are deployed in the IT environment.

The Siebel solution templates provide comprehensive Siebel monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy various performance monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the Siebel solution templates. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the Siebel Solution is available in the SiteScope Siebel Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_Siebel_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Siebel Solution license key from HP.

Solution Template Monitors

The Siebel Solution includes solution templates for monitoring the following key Siebel components:

- **Siebel Application Server for UNIX/Windows.** The SiteScope Siebel Application Server Solutions enable you to monitor the availability, usage statistics, and server performance statistics for Siebel Application servers installed on Windows and UNIX platforms. These solution templates deploy a set of monitors that test the health, availability, and performance of Siebel 6.x, 7.x, and 8.x application servers.
- **Siebel Gateway Server for UNIX/Windows.** The SiteScope Siebel Gateway Server Solutions enable you to monitor the availability and server statistics for Siebel Gateway Servers installed on Windows and UNIX platforms. These solution templates deploy a set of monitors that test the health, availability, and performance of Siebel Gateway Servers. You can use these solution templates to deploy monitors for server-wide resources and metrics.
- **Siebel Web Server for UNIX/Windows.** The SiteScope Siebel Web Server Solutions enable you to monitor the availability and server statistics for Siebel Web servers installed on Windows and UNIX platforms. These solution templates deploy a set of monitors that test the health, availability, and performance of Siebel Web Servers.

Tasks

How to Deploy the Siebel Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Siebel Solution Template.

This task includes the following steps:

- "Prerequisites" on page 1244
- "Deploy the solution template" on page 1246
- "Enter deployment values for the solution template" on page 1246

1 Prerequisites

For the Siebel Application Server solution template:

- The Siebel Server Manager client must be installed only on a Windows machine where SiteScope is running or that is accessible to the SiteScope machine (even if the Siebel application server is installed on UNIX). There are several options for how you can do this. See the documentation for the Siebel Server Manager Monitor for more information.
- You must know the install path for the Server Manager client to be able to setup Siebel Server Manager monitors in SiteScope. If the client is installed on the machine where SiteScope is running, this is the path on that machine. If the client is installed on a remote machine, you must know the fully qualified path to the client executable relative to that machine.
- You must know the name of the Siebel applications that are available in your network. For example, call center, sales, and so on.
- You must know the Siebel database machine name, user name, password, connection URL, and Database Driver.

- You must know the user and password that SiteScope uses for logging into the Siebel server. This user must be granted Siebel Administrator responsibility on the Siebel server.
- You must make sure that the following Siebel server component groups are enabled:
  - Siebel Call Center (CallCenter)
  - Siebel Remote (Remote)
  - System Management (System)
  - Auxiliary System Management (SystemAux) - Siebel 8.x only
- You need to know a significant list of Siebel system component names and their corresponding aliases. For a listing of component names and aliases, see "Siebel Solution Template Page" on page 1247.

Note: For more information on system and configuration requirements, see the sections on the "Siebel Web Server Monitor Overview" on page 586 and "Database Query Monitor Overview" on page 114. These monitor types that are deployed as part of the Siebel Application Server solution template.

For the Siebel Web Server solution template:

- SiteScope server must be able to connect to the machine where the Siebel Web Server is running.
- Siebel Web Server Solution is designed for use with Siebel running on Microsoft Windows platforms.
- Template assumes that the Siebel Web Server is running on Microsoft Internet Information Server (IIS).

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Siebel solution template. For user interface details, see "Siebel Solution Template Page" on page 1247.

Reference

Siebel Solution Template Page

This page enables you to deploy the Siebel solution templates for monitoring the Siebel 6.x, 7.x, and 8.x Application Server, Siebel Gateway Server, and Siebel Web Server on Windows and UNIX platforms.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required Siebel solution template.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Siebel Solution Templates" on page 1241 ➤ "Template Tree" on page 95

Siebel Application Server

The Main Settings include the following elements for monitoring Siebel Application Server 6.x, 7.x, and 8.x on Windows and UNIX environments:

UI Element (A-Z)	Description
Application	Siebel Application Server machine name.
CG_Auxilary_System_Management_Alias (Siebel 8.x only)	Siebel Auxilary System Management component group alias.
CG_Auxilary_System_Management_Name (Siebel 8.x only)	Siebel Auxilary System Management component group name.
CG_Callcenter_Alias	Siebel CallCenter component group alias.
CG_Callcenter_Name	Siebel CallCenter component group name.

UI Element (A-Z)	Description
CG_System_ Management_Alias	Siebel System Management component group alias.
CG_System_ Management_Name	Siebel System Management component group name.
CP_Callcenter_Alias	Siebel CallCenter component alias.
CP_Callcenter_Name	Siebel CallCenter component name.
CP_Client_ Administration_Alias (Siebel 6.x-7.x only)	Siebel Client Administration component alias.
CP_Client_ Administration_Nam (Siebel 6.x-7.x only)	Siebel Client Administration component name.
CP_eService_Alias	Siebel eService component alias.
CP_eService_Name	Siebel eService component name.
CP_File_System_ Manager_Alias	Siebel File System Manager component alias.
CP_File_System_ Manager_Name	Siebel File System Manager component name.
CP_Server_Manager_ Alias	Siebel Server Manager component alias.
CP_Server_Manager_ Name	Siebel Server Manager component name.
CP_Server_Request_ Broker_Alias	Siebel Server Request Broker component alias.
CP_Server_Request_ Broker_Name	Siebel Server Request Broker component name.
CP_Server_Request_ Processor_Alias	Siebel Server Request Broker component alias.
CP_Server_Request_ Processor_Name	Siebel Server Request Processor component name.

UI Element (A-Z)	Description
Database_Connection_URL	URL to the database connection. **Example:** If the ODBC connection is called test, the URL is 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=<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	Driver used to connect to the database.
Database_PASSWORD	Password for the user name used to access the Siebel database.
Database_Username	User name SiteScope should use to access the Siebel database.
Enterprise	Siebel Enterprise server name.
Gateway	Name of the Siebel Gateway server machine.
PASSWORD	Password for the Siebel Client.
SERVER_LIST	Name of the server where the Siebel Application Server is running.
Server_Logical_Instance_Name	Siebel server logical name.
Server_Manager_Path	Local path to the Siebel server manager client. **Example:** D:\sea703\client\bin.
Siebel_Database_Machine_Name	Siebel database machine name.
Siebel_Disk	Disk drive name where Siebel is installed.

UI Element (A-Z)	Description
Siebel_Root_Dir	Path of the shared Siebel root directory. **Example:** The shared root directory for a Siebel 7.5.2 server would be: sea752.
Username	Siebel Client user name.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

Siebel Gateway Server

The Main Settings include the following elements:

UI Element	Description
Siebel_Root_Dir	Path to the Siebel root directory. This directory should contain at least an Admin Console installation.
Siebel_Disk	Disk drive where the Siebel gateway server is running.
Siebel_Logical_ Instance_Name	Siebel server logical name value (for UNIX only).
SERVER_LIST	Name of the server where the Siebel Gateway Server is running. Do not type backslashes (\\), which indicates a UNC path as part of the name of the server.

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

Siebel Web Server

The Main Settings include the following elements:

UI Element	Description
Application	Siebel application to monitor. **Example:** callcenter_enu. Consult with your Siebel administrator for information about names of the installed Siebel applications.
Siebel_Disk	Disk drive name or drive letter where the Siebel Web server is installed.
Siebel_Root_Dir	Name of the shared Siebel root directory. **Example:** Siebel root directory on Windows: sea752.
Siebel_Logical_ Instance_Name	Siebel server logical name value (for UNIX only).
Username	Siebel Client user name needed to log into the Siebel Web server.

UI Element	Description
Password	Siebel Client password needed to log into the Siebel Web server.
SERVER_LIST	Name of the Siebel Web server machine. 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.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

61

Solaris Host Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

Solaris Host Solution Overview

The Solaris Host solution template is a template that you can use to deploy a collection of monitors configured with default metrics that test the health, availability, and performance of the Solaris host. The template supports the versions of Solaris that are supported by SiteScope. For details, see "System Requirements" in the *HP SiteScope Deployment Guide* PDF.

For UNIX Resource Monitors, you can create a Server-Centric report which displays data from three different metrics about the server being monitored.

Tip: We recommend using solution templates when creating the UNIX Resource Monitor, because the required monitors and metrics are already configured. For more information on generating a Server-Centric report, see "Generating a Server-Centric Report" on page 1324.

The Solaris Host solution template provides comprehensive Solaris operating system monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduces the time to configure and deploy various performance monitors, helps identify both real-time performance bottlenecks and longer term trends, and adds only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the Solaris Host solution template. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the Solaris Host Solution settings is available in the SiteScope Operating System Host Best Practices document. This document can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_OS_Best_Practices.pdf**. This is a password protected document. The password is provided along with the Operating System Host Solution license key from HP.

Solution Template Monitors

The 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

Tasks

How to Deploy the Solaris Host Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the Solaris Host solution template.

Note: The Solaris Host solution template deploys a UNIX Resource Monitor for each target host. This is a supplemental monitor that is required for Server-Centric Report support.

This task includes the following steps:

- "Prerequisites" on page 1257
- "Deploy the solution template" on page 1257
- "Enter deployment values for the solution template" on page 1257

1 Prerequisites

- SiteScope server must be able to connect to the target Solaris host.
- The target server must be added to SiteScope as a UNIX remote machine and should pass the UNIX remote test (**Remote Servers** > **UNIX Remote Servers**). For user interface details, see "New/Edit UNIX Remote Server Dialog Box" on page 610.

Note:

- 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.

---

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the Solaris Host solution template. For user interface details, see "Solaris Host Solution Template Page" on page 1258.

Reference

Solaris Host Solution Template Page

This page enables you to deploy the Solaris solution template.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select **Solaris Host**.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "Solaris Host Solution Templates" on page 1253 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
SERVER_LIST	Name of the server you want to monitor. If the server you want to monitor is not in the list, you must define a connection profile to the server. For the steps you use to create a UNIX connection profile, see "How to Configure SiteScope to Monitor a Remote UNIX Server" on page 598.

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to <**SiteScope root directory**>**logs****silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

62

VMware Host Solution Template

This chapter includes:

Concepts

Tasks

Reference

Concepts

VMware Host Solution Overview

You can use the VMware Host solution template to provide monitoring of different aspects of the VMware host server. This includes monitoring of CPU, memory, network, state, and storage -related counters of the VMware host server and its guest virtual machines.

The VMware Host solution template deploys a set of monitors against a particular VMware VirtualCenter. These monitors encompass best practices monitoring for VMware Host. This template includes the VMware Host State, VMware Host CPU, VMware Host Memory, VMware Host Storage, and the VMware Host Network monitors.

The VMware Host solution template provides comprehensive monitoring without requiring the SiteScope user or the IT organization to be experts on the application. It also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the VMware Host solution template. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the VMware Host Solution is available in the SiteScope VMware Host Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_VMware_Host_Best_Practices.pdf**. This is a password protected document. The password is provided along with the VMware Host Solution license key from HP.

Solution Template Monitors

The VMware Host solution template deploys monitors that target the following aspects of VMware Host performance:

- VMware Host CPU
- VMware Host Memory
- VMware Host Network
- VMware Host Storage
- VMware Host State

Tasks

How to Deploy the VMware Host Solution Templates

This task describes the steps involved in entering variables for the VMware Host solution template.

This task includes the following steps:

- "Deploy the solution template" on page 1264
- "Enter deployment values for the solution template" on page 1264

1 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

Note: When a browsable monitor is deployed in a template, the number of counters that match the selected patterns are limited by the **_maxCountersForRegexMatch** parameter in the **master.config** file (this is in addition to the **_browsableContentMaxCounters** parameter which limits the number of counters that browsable monitors can have). If during deployment, the number of counters that match the patterns exceeds this value, only the number of counters up to this value is saved. We recommend using the same value for both these parameters (the default value for both of these parameters is 1000).

---

2 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the VMware Host solution template. For user interface details, see "VMware Host Solution Template Page" on page 1265.

Reference

VMware Host Solution Template Page

This page enables you to deploy the SiteScope VMware Host solution templates.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required VMware Host solution template.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "VMware Host Solution Template" on page 1261 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
VirtualCenter URL	URL of the VMware VirtualCenter infrastructure for the server you want to monitor.
User name	User name of the VMware vCenter service's administrator.
Password	Password of the VMware VirtualCenter service's administrator.
Host	Name of the VMware host server you want to monitor.

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

63

WebLogic Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

WebLogic Solution Overview

The WebLogic solution templates are templates that you can use to deploy a collection of WebLogic Monitors configured with default metrics. The monitors test the health, availability, and performance of a WebLogic Application Server and its deployed applications and components. The deployed monitors check server-wide statistics such as memory usage, as well as metrics specific to individual J2EE components, such as the number of activates and passivates of a particular EJB.

Use the WebLogic Solution to monitor statistics from WebLogic 6.x, 7.x, 8.x, 9.x, and 10.x servers. This solution automatically creates several groups by default which monitor important application server metrics, but it also provides a user interface that enables you to select all or some of the individual components that are available for monitoring.

The WebLogic Solution monitor deployment process is highly customizable in that it enables you to select the specific J2EE components on an application server which SiteScope should actively monitor.

The WebLogic solution templates provide comprehensive WebLogic monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the WebLogic solution templates. Contact your HP sales representative for more information about Solution licensing.
- An in-depth description of the WebLogic solution is available in the SiteScope WebLogic Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\SiteScope_WebLogic_Best_Practices.pdf**. This is a password protected document. The password is provided along with the WebLogic Solution license key from HP.

Solution Template Monitors

The WebLogic solution templates deploy monitors that target the following aspects of WebLogic performance and health:

- **Server Performance Statistics.** This category refers to a collection of server-wide resources that are exposed through the management interface of a WebLogic Application Server.
- **Application Performance Statistics.** Metrics for all of your deployed applications, EJBs, web applications, and servlets are available for monitoring through the WebLogic Solution. The user is responsible for selecting which of these J2EE components he would like to have monitors automatically deployed for. A set of metrics based on WebLogic best practices are monitored for each selected J2EE component.
- **WebLogic Solution Metrics.** For the list of components that can be monitored, see the SiteScope WebLogic Best Practices document.

Tasks

How to Deploy the WebLogic Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the WebLogic solution template.

This task includes the following steps:

1 Prerequisites

The WebLogic solution template deploys a WebLogic Application Server Monitor for each module that is selected from the user interface. This monitor uses the Java JMX interface to access Runtime MBeans on the WebLogic server. An MBean is a container that holds the performance metrics. You may need to set certain permissions on the WebLogic server for SiteScope to be able to monitor MBeans. For an overview on configuring access to WebLogic servers for SiteScope monitors, see "WebSphere Application Server Monitor Overview" on page 830 in the *SiteScope Monitor Reference*.

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the WebLogic solution template. For user interface details, see "WebLogic Solution Template Page" on page 1274.

4 Select WebLogic modules for monitoring

For a brief description of the metrics that are monitored for each type of EJB monitoring, see "Selecting WebLogic Modules for Monitoring" on page 1272.

Reference

 Selecting WebLogic Modules for Monitoring

The WebLogic Solution presents a hierarchical list from which the user can select the modules to deploy WebLogic Monitors against. This list is broken down into two main sections:

- per-server resources
- J2EE components organized by application

Some of the modules in these categories are automatically selected by default because they represent critical components in the system (for example, the JVM statistics for the application server). The remainder of the modules are not automatically selected. This enables you to customize the deployment of this solution to focus on one application, a particular type of EJB, a set of servlets and web applications, or some other aspect of the application server.

For the most part, the organization of this list of modules is intuitive. The hierarchy of applications, EJBs, web applications, and servlets is very similar to the organization of these entities in the WebLogic Administration Console. In almost every case, selecting a module causes a monitor with all relevant metrics to be deployed against that part of the WebLogic server. However, when selecting EJBs to monitor, you notice that they are broken down according to three types of metrics: Pool, Transaction, and Cache. The reason for this is twofold: (1) it is more useful to be able to monitor one aspect of a particular EJB instead per WebLogic Monitor for purposes of alerting and organization, and (2) not all three of these types of metrics are available for all EJBs.

Below is a brief description of the metrics that are monitored for each type of EJB monitoring:

- **Per-EJB Transaction Statistics.** This category of EJB monitor contains metrics related to transactions made for the EJB. These metrics include the number of transactions rolled back, the number of transactions that timed out, and the number of transactions that were successfully committed.
- **Per-EJB Pool Statistics.** This category of EJB monitor contains metrics related to the pool for the EJB. When the user selects an EJB under this heading, many useful metrics are monitored, including the number of times an attempt to get a bean instance from the pool failed, the number of current available instances in the pool, the number of threads currently waiting for an instance, and the number of times a bean instance was destroyed due to a non-application exception.
- **Per-EJB Cache Statistics.** The cache statistics include any metrics relating to the caching of the particular EJB. Metrics like the number of cache hits and misses, and the number of activates and passivates of the EJB are monitored when an EJB under this heading is selected for monitoring.

When you have finished making your module selections in the popup window, scroll to the bottom of the Module Selection window and click the **Select Modules** button. This updates the main browser window with a list of the modules you selected. You can then review your selections and remove any modules that you don't want a monitor to be created for.

When you are satisfied with the list of selected modules in the main browser window, click **Submit**.

WebLogic Solution Template Page

This page enables you to deploy the WebLogic solution template for monitoring Oracle WebLogic 6.x, 7.x, 8.x, 9.x, and 10.x application servers.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required WebLogic solution template.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "WebLogic Solution Templates" on page 1267 ➤ "Template Tree" on page 95

WebLogic 9.x-10.x

The Main Settings include the following elements:

UI Element	Description
WEBLOGIC_URL	URL for the WebLogic 9.x or 10.x application server. **Default value:** 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 or 10.x.
Counters	Displays the server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Opens the Get Counters dialog box, enabling you to select the counters you want to monitor.

UI Element	Description
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

WebLogic 6.x, 7.x, 8.x

The Main Settings include the following elements:

UI Element	Description
WEBLOGIC_PORT	Port number that the WebLogic server is responding on. **Default value:** 7001
WEBLOGIC_ PASSWORD	Password required to log into the WebLogic server.
WEBLOGIC_ USERNAME	User name required to log into the WebLogic server.
WEBLOGIC_ SERVER	Name or address of the server where WebLogic is running.
WEBLOGIC_ TIMEOUT	Number of seconds to wait for a data request to arrive at the WebLogic server. **Default value:** 180

UI Element	Description
WEBLOGIC_JAR_FILE	Absolute path to the weblogic.jar file on the SiteScope machine. This file must be installed on the SiteScope server and can be downloaded from the WebLogic server. **Example:** c:\bea\weblogic7\ebcc\lib\ext\weblogic.jar.
Counters	Displays the server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Opens the Get Counters dialog box, enabling you to select the counters you want to monitor.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

64

WebSphere Solution Templates

This chapter includes:

Concepts

Tasks

Reference

Concepts

WebSphere Solution Overview

The WebSphere solution templates are templates that you can use to deploy a collection of WebSphere Monitors configured with default metrics. The monitors test the availability, server statistics, and deployed J2EE components for IBM WebSphere Application Server 5.x and 6.x. You can use this solution template to deploy monitors for server-wide resources and metrics (for example, thread pool and JVM metrics). You can also create monitors for the deployed EJBs, Web Applications, and Servlets using this solution template.

The WebSphere Solution monitor deployment process is highly customizable in that it enables you to select the specific J2EE components on an application server which SiteScope should actively monitor.

The WebSphere solution templates provide comprehensive WebSphere monitoring without requiring the SiteScope user or the IT organization to be experts on the application. They also reduce the time to configure and deploy monitors, help identify both real-time performance bottlenecks and longer term trends, and add only minimal overhead to production systems.

Note:

- You must have the applicable SiteScope option license to use the WebSphere solution templates. Contact your HP Sales representative for more information about Solution licensing.
- An in-depth description of the WebSphere Solution is available in the SiteScope WebSphere Best Practices document. This document is part of the SiteScope installation, and can be found at **<SiteScope root directory>\sisdocs\pdfs\ SiteScope_WebSphere_Best_Practices.pdf**. This is a password protected document. The password is provided along with the WebSphere Solution license key from HP.

Solution Template Monitors

The WebSphere solution templates deploy monitors that target the following aspects of WebSphere performance and health:

- **Server Performance Statistics.** This category refers to a collection of server-wide resources that are exposed through the management interface of a WebSphere Application Server.
- **Application Performance Statistics.** Metrics for all of your deployed applications, EJBs, web applications, and servlets are available for monitoring through the WebSphere Solution. The user is responsible for selecting which of these J2EE components he would like to have monitors automatically deployed for. A set of metrics based on WebSphere best practices are monitored for each selected J2EE component.
- **WebSphere Application Server Solution Metrics.** For the list of components that can be monitored, see the SiteScope WebSphere Best Practices document.

Tasks

How to Deploy the WebSphere Solution Template

This task describes the steps involved in configuring the server environment and entering variables for the WebSphere solution template.

This task includes the following steps:

1 Prerequisites

The WebSphere server environment must be configured according to the environment being used. For details, see "WebSphere Application Server Monitor Overview" in the *Monitor Reference*.

Note: By default, the WebSphere 6.x Application Server solution template uses the internal JVM mechanism. Accordingly, when using this solution template you should configure the monitoring environment to use internal Java. For details, see "Configure the WebSphere 6.0x Server Environment Using Internal Java" on page 839 and "Configure the WebSphere 6.1x Server Environment Using Internal Java" on page 846.

---

2 Deploy the solution template

For a detailed overview of the steps involved in deploying a solution template, see "How to Deploy a SiteScope Solution Template" on page 1088.

3 Enter deployment values for the solution template

Complete the items on the Deployment Values page for the WebSphere solution template. For user interface details, see "WebSphere Solution Template Page" on page 1282.

Reference

WebSphere Solution Template Page

This page enables you to deploy the WebSphere solution template for monitoring IBM WebSphere Application Servers 5.x and 6.x.

To access	Select the **Templates** context. In the template tree, expand **Solution Templates**, and select the required WebSphere solution template.
Relevant tasks	"How to Deploy a SiteScope Solution Template" on page 1088
See also	➤ "WebSphere Solution Templates" on page 1277 ➤ "Template Tree" on page 95

Main Settings

User interface elements are described below:

UI Element	Description
WEBSPHERE_ SERVER	Name of the server where the WebSphere Application is running. Do not type backslashes (\\) that indicate a UNC path as part of the name of the server.
WEBSPHERE_ PORT	Port number of the WebSphere server. This should be the SOAP port for WebSphere 5.x. **Default value:** 8880

UI Element	Description
WEBSPHERE_USER_NAME	User name that SiteScope should use to log on to the 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 Monitor Settings pane, update the Global Security boxes (**Trust store**, **Trust store password**, **Key store**, **Key store password**).
WEBSPHERE_PASSWORD	Password that SiteScope should use to log on to the 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 Monitor Settings pane, update the Global Security boxes (**Trust store**, **Trust store password**, **Key store**, **Key store password**).
WEBSPHERE_CLIENT_PROPERTIES_FILE	The client properties file. **Default value:** /properties/soap.client.props
WEBSPHERE_DIRECTORY	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_VERSION (WebSphere 6.x solution only)	Select the WebSphere version when using the WebSphere 6.x solution template (6.0x or 6.1x).

UI Element	Description
WEBSPHERE_USE_EXTERNAL_JVM	Enables using external JVMs for monitoring. By default, the WebSphere monitor uses internal JVMs. External JVMs consume greater resources, take longer to start up, and have bad error handling. **Note:** You cannot use certificates added using Certificate Management if external JVMs are used. **Default value:** false
Counters	Displays the server performance counters you want to check with this monitor. Use the **Get Counters** button to select counters.
Get Counters	Opens the Get Counters dialog box, enabling you to select the counters you want to monitor.
Silent deployment	Submits the template deployment request to a queue, and SiteScope handles the deployment in the background. This enables you to continue to use SiteScope without having to wait for the template deployment process to finish. All submitted requests and their corresponding deployment results are logged to **<SiteScope root directory>\logs\silent_deployment.log**. **Default value:** Not selected
Verify monitor properties with remote server	Verifies the correctness of the monitor configuration properties in the template against the remote server on which the template is deployed. **Note:** When this option is selected, deployment time is slowed due to the remote connection. **Default value:** Selected

Part X

SiteScope Dashboard

65

Working with SiteScope Dashboard

This chapter includes:

Concepts

Tasks

Reference

Concepts

SiteScope Dashboard Overview

SiteScope monitoring provides a real-time picture of system availability and performance. You configure SiteScope monitors to collect metrics from a range of infrastructure components, including Web, application, database, and firewall servers. The status and metrics are then aggregated for presentation in SiteScope Dashboard.

Dashboard is linked to the SiteScope monitor tree hierarchy. The data displayed in Dashboard represents the selected context in the monitor tree. The highest level is the SiteScope node and any applicable monitor groups. The lowest-level element for display in a Dashboard view is an individual SiteScope monitor and its measurements.

Dashboard includes functions that you can use to customize the display of monitor information. This includes defining named filter settings to limit the display of data to those matching a defined criteria. You can also select various data display options.

Dashboard also includes hyperlinks and menus that you can use to navigate through the hierarchy of monitor elements, manually run a monitor, disable monitors, and access alert definitions.

Dashboard Filter Overview

You can filter monitors or groups by the following criteria:

- Monitor or group names containing a specific text string.
- Monitors or groups monitoring a specific host or server.
- Monitors or groups reporting an error.
- Measurement results containing a specific text string.

Filters are applied primarily to monitors. The filter criteria are not applied to groups, alerts, or reports. You can use view settings to filter on other elements. For more information, see "Searching and Filtering SiteScope Objects Overview" on page 116.

Filters are applied to all Dashboard views. This means that some monitors may not be displayed depending on the filter criteria and the selected node. Generally, it is best to use filters together with the **Show All Descendent Monitors** view option. Filters remain active until you change or reset the filter criteria in the Dashboard Filter window.

Dashboard filters are separate from SiteScope tree filters. You can use either Dashboard filters or SiteScope tree filters to filter the display of nodes to specific monitor types. However, Dashboard filters are applied to the results of any currently selected tree filter setting. If a tree filter setting is active, this may prevent the Dashboard filter from finding monitors that match the filter criteria, even if such monitors do exist in the SiteScope environment.

You can save a filter setting by defining the filter settings and then saving the view as a Dashboard Favorite. For more information, see "Defining and Managing Filter Settings" on page 117.

For details on configuring a Dashboard filter, see "Dashboard Filter Dialog Box" on page 1312.

Acknowledging Monitor Status

The acknowledgement function can be used to track resolution of problems that SiteScope detects in your system and network infrastructure. With this function, SiteScope keeps a record of when the problem was acknowledged, what actions have been taken, and by which user.

It also enables you to temporarily disable alerting on the monitors. This is useful to avoid redundant alerts while a problem is being actively addressed. You can also use the acknowledgement function as a simple trouble ticket system when more than one person uses SiteScope to manage system availability.

Note: The acknowledgement function is available only in Dashboard views. The acknowledgement icon is displayed only in Dashboard Detailed views.

You can add an acknowledgement to individual monitors or monitor groups. An acknowledgement added to a monitor applies only to that monitor. Any alert disable condition selected in the acknowledgement applies only to that monitor instance. Acknowledging a group applies the acknowledgement description and alert disable conditions to all monitors within the group. Acknowledgements applied to a group can be edited or deleted individually for monitors in the group.

Only one acknowledgement can be in force for a monitor or group at any given time. Acknowledgement comments and acknowledgement indicators continue to be displayed in the interface until they are deleted, even after any applicable alert disable schedule has expired.

Acknowledgement data and comments are written to a log file on the SiteScope machine. A new log entry is made each time you add, edit, or delete an acknowledgement. After a problem monitor or group is acknowledged, or the acknowledged status is cleared, you can view the history in the Acknowledge Log. The Acknowledge Log for an item can be viewed even if there is no acknowledgment currently in force.

For details on the Add Acknowledgment user interface, see "Acknowledge Monitors In Group Dialog Box" on page 1308.

Accessing SiteScope Tools

SiteScope contains a number of tools that can be used to test the monitoring environment. You can use these tools to query the systems you are monitoring and view detailed results of the action. This may include simply testing network connectivity or verifying login authentication for accessing an external database or service. You can run these tools directly from the Dashboard toolbar by clicking the **Tools** button for the monitor (if diagnostic tools are available for the specific monitor).

For details on the different tools that are available, see "SiteScope Tools Overview" on page 160.

Note: SiteScope Tools option is available only for individual monitors.

Tasks

How to Customize SiteScope Dashboard

This task describes the steps involved in customizing the display and content of SiteScope Dashboard by setting the layout, configuring filters, and saving the view to favorites.

This task includes the following steps:

- "Set the Dashboard layout" on page 1292
- "Select and set a Dashboard filter - optional" on page 1292
- "Save view to favorites" on page 1293

1 Set the Dashboard layout

Customize the display of group and monitor information using the settings on the Dashboard Settings dialog box.

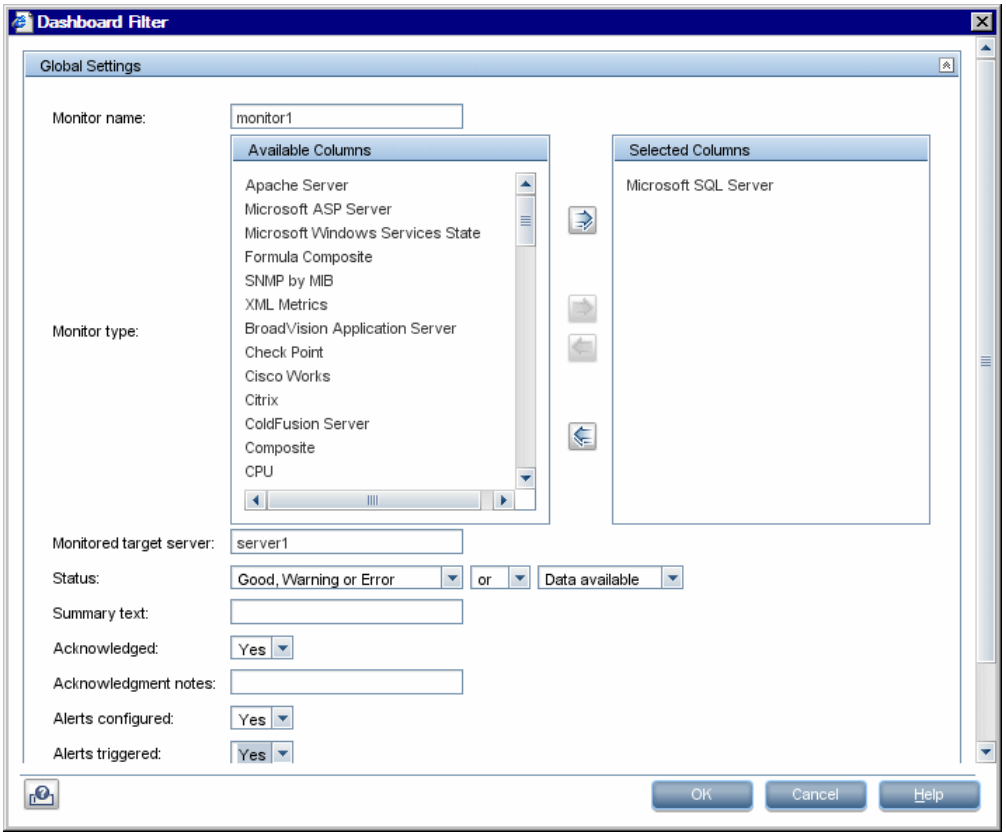
For user interface details, see "Dashboard Settings Dialog Box" on page 1316.

2 Select and set a Dashboard filter - optional

Configure and set a Dashboard filter by selecting from the options available on the Dashboard Filter dialog box.

For user interface details, see "Dashboard Filter Dialog Box" on page 1312.

Example:



3 Save view to favorites

After defining the Dashboard filter and layout settings, you can save them as a named favorite view in the Favorites list by clicking the arrow next to the **Manage Favorites** button, and selecting **Save to Favorites**.

For user interface details, see "Save to Dashboard Favorites Dialog Box" on page 1310.

How to Analyze Data in SiteScope Dashboard

This task describes the steps to follow to analyze data in SiteScope Dashboard.

This task includes the following steps:

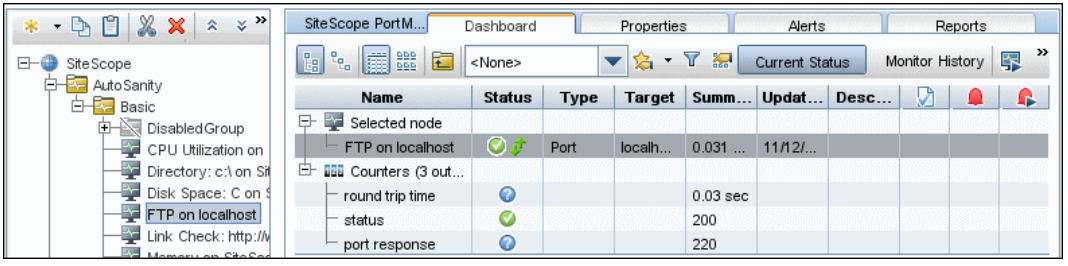
- "Drill down to view monitor and measurement status and availability" on page 1294
- "View configured and triggered alerts" on page 1295
- "Acknowledge monitors" on page 1295
- "Monitor your Microsoft Windows/UNIX server's resources" on page 1296
- "View monitor history" on page 1296

1 Drill down to view monitor and measurement status and availability

When viewing SiteScope data in the Current Status view of Dashboard, you can drill down in the monitor tree to view monitor and measurement status and availability.

For user interface details, see "SiteScope Dashboard - Current Status View" on page 1298.

Example:

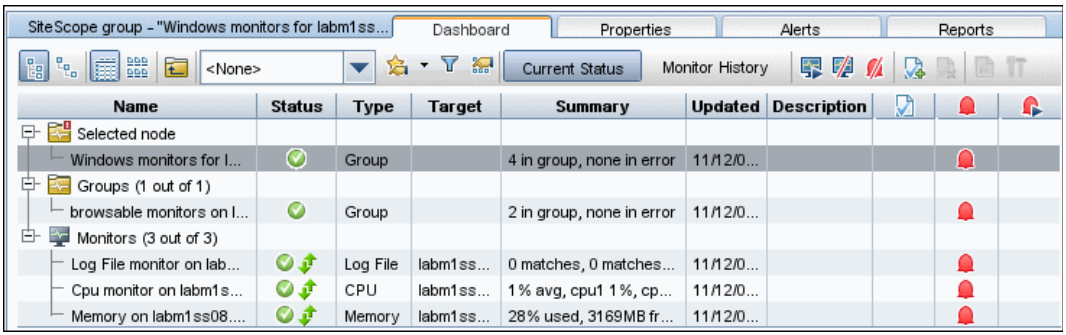


2 View configured and triggered alerts

You can view data about alerts in the configured alerts and triggered alerts columns. If alerts are configured for a monitor, you can double-click the **Configured Alert** icon to see the list of configured alerts, and select an alert to view or edit the alert properties.

For user interface details, see "SiteScope Dashboard - Current Status View" on page 1298.

Example:

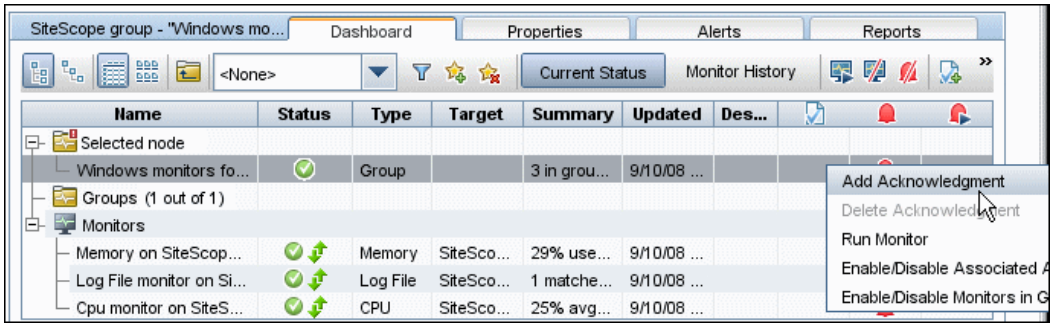


3 Acknowledge monitors

To acknowledge monitor status, click the **Add Acknowledgment** icon or select **Add Acknowledgment** from the context menu, and enter the details in the Acknowledge Monitors In Group dialog box.

For user interface details, see "Acknowledge Monitors In Group Dialog Box" on page 1308.

Example:



4 Monitor your Microsoft Windows/UNIX server's resources

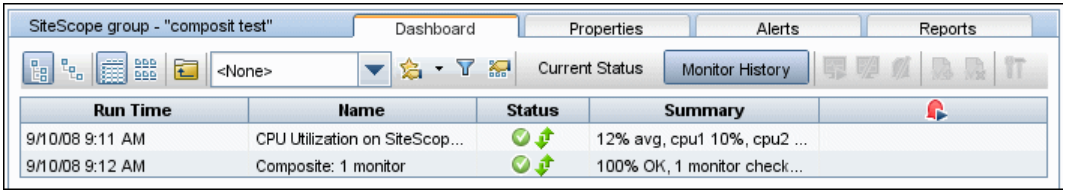
You can create a Microsoft Windows or UNIX Resources monitor to monitor your Windows or UNIX Server, and generating a Server-Centric report. For task details, see "How to Create a Server-Centric Report" on page 1326.

5 View monitor history

You enable and configure monitor history in the General Preferences. For user interface details, see "Dashboard Monitor History View Options" on page 704.

To view monitor history, click the **Monitor History** button in SiteScope Dashboard. For user interface details, see "SiteScope Dashboard - Monitor History View" on page 1307.

Example:



Reference

SiteScope Dashboard User Interface

This section includes:

SiteScope Dashboard - Current Status View

Displays current performance data for the infrastructure elements being monitored by SiteScope and provides access to functions you use to define filters. The Dashboard displays a table of groups and monitors for the element highlighted in the monitor tree or listed in the path. You can double-click each group or monitor node to navigate to child nodes and monitors.

From the Dashboard, you can access Server-Centric reports, preconfigured Quick reports, acknowledge monitor status, monitor tools, SiteScope Health Status, monitor history information, and enable/disable monitors and alerts.

To access	Select the **Monitors** context. Select an object in the monitor tree, and click the **Dashboard** tab in the right pane.
Important information	➤ By default, the maximum number of objects that can be displayed in the Dashboard table for a selected element is 4000, and the maximum number of icons that can be displayed in Icon View is 700. You can modify these numbers by changing the values in the Dashboard Settings dialog box. However, we recommend that you use the default setting. ➤ If the selected element has more lines than the maximum number that can be displayed in the Dashboard table, try creating a more restrictive tree filter or configure a Dashboard filter.
Relevant tasks	➤ "How to Customize SiteScope Dashboard" on page 1292 ➤ "How to Analyze Data in SiteScope Dashboard" on page 1294
See also	"SiteScope Dashboard Overview" on page 1288

User interface elements are described below:

UI Element	Description
	**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.
	**Show All Descendent Monitors.** Displays all descendent monitors of the selected node. When the Icon view option is selected, only descendent monitor icons and names are displayed.
	**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.
	**Up.** Goes up one level in the monitor tree. This option is not available for SiteScope (the highest level in the tree).
	The Favorite box contains a drop-down list of the existing favorite views of Dashboard filter and layout settings. You can select the one you want to display in the Current Status or Monitor History view. **Note:** The Favorites filter works on the monitor level which means that it does not filter groups. When working in the **Show Child Groups and Monitors** view, you can see groups that are not in a state that match the filter. To see only monitors in the filter, use the **Show All Descendent Monitors** view instead. **Default value:** <None>

UI Element	Description
	**Manage Favorites.** Click the arrow, and select an option: ➤ **Save to Favorites.** Opens the Save to Dashboard Favorites dialog box which enables you to save the current Dashboard filter and layout settings as a favorite view. For user interface details, see "Save to Dashboard Favorites Dialog Box" on page 1310. ➤ **Delete Favorites.** Opens the Delete Dashboard Favorites dialog box which enables you to delete existing favorite views. For user interface details, see "Delete Dashboard Favorites Dialog Box" on page 1311.
	**Dashboard Filter.** Opens the Dashboard Filter dialog box. For user interface details, see "Dashboard Filter Dialog Box" on page 1312.
	**Dashboard Settings.** Opens the Dashboard Settings dialog box. For user interface details, see "Dashboard Settings Dialog Box" on page 1316.
	**Current Status.** Displays a table of groups and monitors for the element highlighted in the monitor tree or listed in the path.
	**Monitor History.** 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. For more information on viewing monitor history, see "SiteScope Dashboard - Monitor History View" on page 1307.
	**Run Monitors.** Runs the monitor or any monitors configured in the group. This opens an information window with the results.

UI Element	Description
	**Enable/Disable Monitors in Group.** Opens the Enable/Disable Monitors in Group dialog box which enables you to enable or disable the monitor or all the monitors in the group, regardless of the setting in the monitor properties. If you select **Disable monitor**, the monitors are disabled until you return to this dialog box and select **Enable monitor**. For details on the Enable/Disable Monitors in Group user interface, see "Enable/Disable Monitors in Group Dialog Box" on page 1321.
	**Enable/Disable Associated Alerts.** Opens the Enable/Disable Associated Alerts dialog box which enables you to enable or disable all alerts associated with the monitor or all monitors in the group. For more details, see "Enable/Disable Associated Alerts" on page 482
	**Add Acknowledgment.** Opens the Acknowledge Monitors In Group dialog box which enables you to add an acknowledgment to a monitor. For details on the Acknowledge Monitors In Group user interface, see "Acknowledge Monitors In Group Dialog Box" on page 1308.
	**Delete Acknowledgment.** Deletes the monitor's acknowledgment.
	**Quick Report.** Creates a one-time SiteScope management report using preconfigured settings for the selected monitor. For more details on the report, see "Quick Report" on page 1542.
	**Tools.** Opens a diagnostic tool to test the selected monitoring environment. This button is available only for those monitor instances for which there is an appropriate diagnostic tool. For details on the SiteScope Tools, see "Diagnostic Tools" on page 1319.

UI Element	Description
	**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 acknowledgment information as a tool tip. Double-click the icon to open the Edit Acknowledge dialog box. For details on this topic, see "Acknowledging Monitor Status" on page 1290. For details on the Add/Edit Acknowledge dialog box, see "Acknowledge Monitors In Group Dialog Box" on page 1308.
	**Configured Alerts** column. Indicates that one or more alerts are associated with the group or monitor. If you double-click the icon, a tooltip displays the configured alerts. Selecting an applicable alert definition name from the list opens the Edit Alert dialog box enabling you to view or edit the alert properties. For details on this topic, see "SiteScope Alerts" on page 1415.
	**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. For a list of icons, see "Alert Actions" on page 1465. If multiple alerts were triggered, an icon representing multiple alerts is displayed. Clicking the alert icon displays alert details. The Triggered Alert column only appears for a table that contains monitors. For details on this topic, see "SiteScope Alerts" on page 1415.
<Objects table>	Lists the groups and monitors for the element highlighted in the monitor tree or listed in the path. You can double-click each group or monitor node to navigate to child nodes and monitors. Double-click a monitor to display the performance counters for that monitor.

UI Element	Description
Name	A display name (alias) for the monitor instance or group. When a new group is created, you type its name. When a new monitor is created, you select its type from the list of available monitors. If you do not override this type in the **Name** box, the monitor is identified by the type of monitor. You can then optionally type an alias that helps you identify this monitor.
Status	A colored icon is displayed for each node in a Dashboard view, representing the operational status assigned to that component for its current performance level. A color-coded arrow is also displayed for each element in a Dashboard view, representing the data availability status of the monitor. You can point at the icons to display the monitor status and availability. For a description of the monitor status and availability icons, see "Status and Availability Levels" below.
Type	The type of monitor being displayed. You select the monitor type in the New Monitor dialog box when you create the monitor instance.
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** box when the server was added to the monitor tree. If the group contains a Microsoft Windows Resources monitor or UNIX Resources monitor, the server name in the Target column appears as a link. You can click the link to open the Server-Centric report for the server. For user interface details, see "Server-Centric Report" on page 1323.

UI 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. If a monitor has been disabled, it displays the disabled status (disabled manually, disabled until x time, or disabled by <Downtime Name> from BSM).
Updated	The date and time when the last event occurred in the group or monitor.
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 the link. If this field contains text, you can double-click it to open a dialog box that displays the full description in HTML format. You can enter information in this column by selecting the monitor or group in the monitor tree and selecting the **Properties** tab. In the page that opens, expand **General Settings** and enter a description in the **Monitor/Group description** box.

Status and Availability Levels

Icon	Description
	**Good Status**. All performance measurements are within the Good threshold level.
	**Warning Status**. At least one performance measurement is within the Warning range, but no measurements are within the Error or Poor range.

Icon	Description
	**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.
	**Status Not Defined (No Data).** There is no data for the group or monitor. This can be caused by any of the following reasons: ➤ A new monitor has not yet run. ➤ Monitor counters have not yet been collected. ➤ The monitors on which the group or monitor depend are not reporting a Good condition.
	**No Thresholds Breached Status.** No thresholds were defined for the monitor counter, so no status is assigned.
	**Disabled Manually.** The group or monitor is currently disabled, and no data updates are being received.
	**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.

Dashboard Shortcut Menu

The following options are available by right-clicking in any column of a group or monitor object row:

UI Element (A-Z)	Description
Add Acknowledgment	Opens the Acknowledge dialog box which enables you to add an acknowledgement to a monitor.
Delete Acknowledgment	Deletes the monitor's acknowledgement.
Enable/Disable Associated Alerts	Opens the Enable/Disable Associated Alert dialog box which enables you to enable or disable all the alerts for all monitors in the group. If you select **Disable monitor**, the alerts are disabled until you return to this page and select **Enable monitor**. For more details, see "Enable/Disable Associated Alerts" on page 482.
Enable/Disable Monitor **Enable/Disable Monitors in Group**	Opens the Enable/Disable Monitor Settings dialog box which enables you to enable or disable the monitor or all monitors in the group. If you select **Disable**, the monitors are disabled until you return to this page and select **Enable**. For user interface details, see "Enable/Disable Monitors in Group Dialog Box" on page 1321.
Quick Report	Creates a one-time SiteScope management report using preconfigured settings for the selected monitor. For more details, see "Quick Report" on page 1542. **Note:** This menu item is displayed for monitors only.
Run Monitor(s)	Runs the selected monitor or all monitors in the selected group.
Tools	Opens a diagnostic tool that can help you troubleshoot monitor configuration problems. For details on the available tools, see "SiteScope Tools Overview" on page 160. **Note:** This menu item is displayed for monitors only, and is available for specific monitors only.

SiteScope Dashboard - Monitor History View

This view displays information about monitors, monitor groups, and alerts collected during the last 24 hours. This information is filtered by the number of hours, monitor status, and the number of data entries.

To access	Select the **Monitors** context. In the Dashboard toolbar, click the **Monitor History** button.
Important information	➤ You enable this function by selecting **Enable monitor history view** in **Preferences** > **General Preferences** > **Dashboard Monitor History View Options**. ➤ You can determine exactly how much data you want saved for this function so that your database does not get overloaded. ➤ By default, the maximum number of objects that can be displayed in the Monitor History table for a selected element is 4000, and the maximum number of icons that can be displayed in Icon View is 70. You can modify these numbers by changing the values in the Dashboard Settings (select **Monitors**, click the **Dashboard Settings** button, and expand **Dashboard Properties**). However, we recommend that you use the default setting. For details, see "Dashboard Settings Dialog Box" on page 1316. ➤ If the selected element has more lines than the maximum number that can be displayed in the Monitor History table, try creating a more restrictive tree filter or configure a Dashboard filter.
Relevant tasks	➤ "How to Customize SiteScope Dashboard" on page 1292 ➤ "How to Analyze Data in SiteScope Dashboard" on page 1294
See also	"Dashboard Monitor History View Options" on page 704

User interface elements are described below:

UI Element	Description
	**Triggered Alert.** Appears next to any monitor that triggered an alert.
Run Time	Time the monitor ran.
Name	Name of the monitor.
Status	The monitor's status at runtime (Error, Warning, or Good). For user interface details, see "Status and Availability Levels" on page 1304.
Summary	Description of the monitor run.

Acknowledge Monitors In Group Dialog Box

This dialog box enables you to add or edit an acknowledgement for a monitor or monitor group.

To access	Select the **Monitors** context. In the monitor view, right-click a monitor or group, and select: ➤ **Add Acknowledgment** to add an acknowledgement to individual monitors or a monitor groups. ➤ **Edit Acknowledgment** to edit an acknowledgment for a monitor or group that has been acknowledged.
Relevant tasks	➤ "How to Customize SiteScope Dashboard" on page 1292 ➤ "How to Analyze Data in SiteScope Dashboard" on page 1294
See also	"Acknowledging Monitor Status" on page 1290

User interface elements are described below:

UI Element	Description
Acknowledge comment	An acknowledgement comment which is displayed as a tooltip associated with the acknowledgment icon in the Dashboard view and is recorded in the Acknowledge Log. You can update the comment as new information becomes available. The comment is displayed until the acknowledgment is deleted.
Enable all associated alerts	Enables all associated alerts (default setting).
Disable all associated alerts for the next <time period>	Disables alerting immediately and to continue suppressing alerting on the selected monitor or group for a duration that you specify.
Disable all associated alerts on a one time schedule from <timeA> to <timeB>	Disables alerting during a period of time that you specify. This can be useful if the system being monitored is expected to be unavailable during a certain period but you want to continue to run the monitor without triggering an alert.
Disable description	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.
View Acknowledge Log	View all acknowledgment entries for the monitor or group from which you invoke the acknowledgment dialog box. The log contains the time and date of the acknowledgement, user name of the acknowledger, the status of the monitor or group, and the acknowledgement message.

Save to Dashboard Favorites Dialog Box

This dialog box enables you to define combinations of Dashboard filter and layout settings (which were selected using the Dashboard Filter dialog box and the Dashboard Settings dialog box) and save them as a named favorite view.

To access	Select the **Monitors** context. In the Dashboard toolbar, click the arrow next to the **Manage Favorites** button, and select **Save to Favorites**.
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.
Relevant tasks	"How to Customize SiteScope Dashboard" on page 1292
See also	"SiteScope Dashboard Overview" on page 1288

User interface elements are described below:

UI Element	Description
Name	Select an option for saving the current Dashboard filter and layout settings to favorites: ➤ **Existing.** Enables you to replace one of the existing favorites with the current settings. Displays a list of the existing favorite views. By default, the list includes all the preconfigured favorites. ➤ **New.** Enables you save the current settings to a new favorite view with the display name that you enter in the box.

Delete Dashboard Favorites Dialog Box

This dialog box enables you to delete existing favorite views

To access	Select the **Monitors** context. In the Dashboard toolbar, click the arrow next to the **Manage Favorites**  button, and select **Delete Favorites**.
Relevant tasks	"How to Customize SiteScope Dashboard" on page 1292
See also	"SiteScope Dashboard Overview" on page 1288

User interface elements are described below:

UI Element	Description
Existing Favorites	Select the view or views you want to delete from the list of current favorite views. By default, the list includes the following preconfigured favorites: ➤ All Objects ➤ Disabled ➤ Errors Only ➤ Errors and Warnings ➤ Good ➤ Good and Warnings ➤ No Data ➤ Warnings Only

Dashboard Filter Dialog Box

This dialog box enables you to configure a Dashboard filter by entering match criteria and selecting from the menu options.

To access	Select the **Monitors** context. In the Dashboard toolbar, click the **Dashboard Filter** button.
Important information	Any combination of filter options can be included in a single filter. For example, the filter definition can filter on a combination of **Monitor type**, **Monitored target**, and **Status**.
Relevant tasks	➤ "How to Customize SiteScope Dashboard" on page 1292 ➤ "How to Analyze Data in SiteScope Dashboard" on page 1294
See also	"Dashboard Filter Overview" on page 1289

Global Settings

User interface elements are described below:

UI Element	Description
Monitor name	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	Filters monitors by the selected monitor types.
Monitored target server	Filters monitors by server name on a particular host or monitored server.

UI Element	Description
Status	Filters monitors by reported status. The status filter criterion can be defined in terms of monitor category status. The following status options are available: ➤ **Any Status.** Show all monitors with any status. This is the default option. This can be used in combination with the **Data Available** option to filter out monitors that are in error due to connectivity or availability factors. ➤ **Disabled.** Show only monitors reported as disabled. ➤ **Error.** Show only monitors reporting an error status. ➤ **Good.** Show only monitors reporting a good or OK status. ➤ **Good, Warning, or Error.** Show all monitors except those reported as disabled. ➤ **Warning.** Show only monitors reporting a warning status. ➤ **Warning or Error.** Show only monitors reporting a warning or error status. ➤ **Warning or Good.** Show only monitors reporting a warning or good status. **Example:** Create a filter that displays only those monitors reporting a warning or error.

UI Element	Description
Status (with Availability)	Creates 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	Filters monitors based on text included in their summary string. You can type a literal text string or a regular expression to match a text pattern. For details about regular expressions see "Using Regular Expressions" on page 235.
Acknowledged	Filters monitors based on their Operator Acknowledgment 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.
Acknowledgment notes	Filters monitors based on text that may appear in their Operator Acknowledgment notes. You can type a literal text string or a regular expression to match a text pattern. For details about regular expressions see "Using Regular Expressions" on page 235.

UI Element	Description
Alerts configured	Filters 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	Filters 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.

Monitor History Settings

User interface elements are described below:

UI Element	Description
Display time period	Time frame for past events. **Default value:** Past 1 hour
Monitor run status	Required event status, relational operator, and data availability. **Default value:** Any

Dashboard Settings Dialog Box

This dialog box enables you to customize the display of group and monitor data in the Dashboard views. This enables you to display or suppress the display of monitor measurement details, alert information, and acknowledgement functions.

To access	Select the **Monitors** context. In the Dashboard toolbar, click the **Dashboard Settings** button.
Important information	Layout options apply only to the Detailed view. They are ignored when using the Icon view.
Relevant tasks	"How to Customize SiteScope Dashboard" on page 1292
See also	"Dashboard Filter Overview" on page 1289

Dashboard Table Layout

User interface elements are described below:

UI Element	Description
Lock columns	Locks the order of the table's columns. Clear the setting to change the table column order by dragging the column header to the right or the left. **Default value:** Not selected
Table Columns	Columns displayed in the detailed tables. Your selections are applied to all applicable group and monitor elements. The columns available for display are: ➤ Type ➤ Summary ➤ Alerts Triggered ➤ Alerts Configured ➤ Description ➤ Status ➤ Target ➤ Ack(nowledged) ➤ Updated ➤ Name **Default value:** All the properties are selected For details on the columns, see "SiteScope Dashboard - Current Status View" on page 1298

Dashboard Properties

User interface elements are described below:

UI Element	Description
Show monitor availability	Displays monitor availability icons in the Dashboard that indicate whether SiteScope was able to connect to a remote system or if a remote system was unavailable due to a connection problem. **Default value:** Not selected.
Maximum dashboard objects	Maximum number of objects that can be displayed in the Dashboard table for a selected element. **Default value:** 4000 **Note:** If the selected element has more objects than the maximum number that can be displayed, you should try to create a more restrictive tree filter or configure a Dashboard filter instead of increasing this setting.
Maximum dashboard icons	Maximum number of icons that can be displayed in the Dashboard's Icon View. **Default value:** 700 **Maximum recommended value:** 1500 **Note:** If the selected element has more icons than the maximum number that can be displayed, you should try to create a more restrictive tree filter or configure a Dashboard filter instead of increasing this setting.
Dashboard refresh rate (in seconds)	Amount of time, in seconds, to wait between refreshing the Dashboard. **Default value:** 60 seconds **Minimum value:** 30 seconds

Diagnostic Tools

The SiteScope tools enable you 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.

To access	Select the **Monitors** context. In the Dashboard, select a monitor instance for which a diagnostic tool is available, and click the **Tools** button.
Important information	The **Tools** button is enabled when configuring or viewing the following monitor instances: ➤ Active Directory Replication monitor ➤ Cisco Works monitor ➤ CPU monitor ➤ Database Counter monitor ➤ Database Query monitor ➤ DB2 8.x and 9.x monitor ➤ Disk Space monitor ➤ DNS monitor ➤ F5 Big-IP monitor ➤ FTP monitor ➤ LDAP monitor ➤ Log File monitor ➤ Mail monitor ➤ Memory monitor ➤ Microsoft Windows Event Log monitor ➤ Microsoft Windows Media Player monitor ➤ Microsoft Windows Performance Counter monitor ➤ News monitor ➤ Oracle 9i Application Server monitor ➤ Ping monitor ➤ Port monitor ➤ Real Media Player monitor ➤ Service monitor

Important information (Continued)	➤ SNMP monitor ➤ SNMP by MIB monitor ➤ SNMP Trap monitor ➤ Technology Database Integration monitor ➤ Technology SNMP Trap Integration monitor ➤ URL monitor ➤ URL Content monitor ➤ Web Service monitor ➤ XML Metrics monitor For the complete list of diagnostic tools that are available in SiteScope, click the **Tools** button in the lower left pane.
See also	"SiteScope Tools Overview" on page 160

Enable/Disable Monitors in Group Dialog Box

This dialog box enables you to select an option for enabling or disabling the monitor or all the monitors in the group, regardless of the individual monitor setting in the monitor properties tab. If you select **Disable monitor**, the monitors are disabled until you return to this dialog box and select **Enable monitor**.

To access	Select the **Monitors** context. In the Dashboard, select a monitor or group, and click the **Enable/Disable Monitor** button.
Important information	If you disable a monitor or group using the **Disable monitor** option, the Dashboard shows disabled manually as the status in the **Summary** column for the affected objects. You must enable any object with a disabled manually status before you can set objects to be disabled for a specific period of time. This is also true at the group level. For example, if monitors in a group are disabled for a time period and monitors in a subgroup of that group have the disabled manually status, the subgroup monitors remain disabled even after the disable time period has lapsed for the parent group.
See also	"Enable/Disable Monitor" on page 479

User interface elements are described below:

UI Element	Description
Enable monitor	Enables the monitors if they were previously disabled in the monitor properties. **Default value:** Selected
Enable temporarily disabled monitor only	Enables the monitors if they were previously disabled temporarily in the monitor properties.

UI Element	Description
Disable monitor	When monitors in the group have been disabled, SiteScope continues to schedule the monitors to run based on the **Frequency** setting for the monitor but the monitor action is not run. SiteScope records a monitor data log entry for the monitors when they were scheduled to be run but reports the monitor status as disabled in the place of measurement data.
Disable monitor for the next <time period>	Time period that the monitors should remain disabled. Select **Seconds**, **Minutes**, **Hours**, or **Days** to define the disable time period as applicable.
Disable monitor on a one time schedule from <time> to <time>	Temporarily disables the monitor for a time period in the future. The time period can span more than one day. Enter or select the start time and end time for the disable period using the format: hh:mm:ss mm/dd/yyyy.
Disable description	Descriptive that 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** option.

66

Server-Centric Report

This chapter includes:

Concepts

Tasks

Reference

Concepts

Generating a Server-Centric Report

For Microsoft Windows and UNIX Resources monitors you can create a Server-Centric report which displays data from three different metrics about the server being monitored.

Tip: We recommend using Solution Templates when creating the Microsoft Windows Resources or UNIX Resources monitor. For details on the Solution Templates, see:

- "AIX Host Solution Template" on page 1113
- "Linux Host Solution Template" on page 1157
- "Solaris Host Solution Templates" on page 1253
- "Microsoft Windows Host Solution Template" on page 1207

You can define the monitor manually by selecting **Enable Server-Centric report** in the required monitor settings page, as described in "Microsoft Windows Resources Monitor Settings" on page 416 and "UNIX Resources Monitor Settings" on page 657. 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 1333.

The report displays the following metrics on the same graph:

- **CPU Utilization.** For UNIX Resource Monitors, this metric is calculated as an average of three counters: system processing utilization, user processing utilization, and input/output processing utilization. For Microsoft Windows Resources Monitors, the metric is calculated as processing capacity used out of total processing capacity.
- **Memory Utilization.** Calculated as memory used out of total available memory.

➤ **Network Utilization.** Calculated by system-specific counters. Calculating network utilization is supported only for Windows servers.

Each metric is displayed by a separate line of a unique color on the graph. The report enables you to easily make a visible correlation between the different metrics.

The report includes tables listing the top five processes by CPU utilization and memory consumption. You can navigate the graph and change the time of the data displayed in the tables. This enables you to focus in on a problematic period in the graph to locate the processes running at that time. For details on the Server-Centric report interface, see "Server-Centric Report" on page 1334.

For details on how to generate a Server-Centric report, see "How to Create a Server-Centric Report" on page 1326.

Tasks

How to Create a Server-Centric Report

This task describes the steps involved in creating a monitor to monitor your Windows and UNIX server, and generating a Server-Centric report.

Note: For a scenario of this task, see "How to Create a Server-Centric Report – Use-Case Scenario" on page 1328.

This task includes the following steps:

- "Create a Microsoft Windows or UNIX Resources monitor" on page 1326
- "Generate the Server-Centric report" on page 1327
- "Analyze data in the report" on page 1327

1 Create a Microsoft Windows or UNIX Resources monitor

To monitor your Microsoft Windows or UNIX server, you must create a Microsoft Windows or UNIX Resources monitor. You can create the monitor manually, or by using solution templates (recommended).

- For details on manually creating a Microsoft Windows Resources or UNIX Resources monitor, see:
  - "Microsoft Windows Resources Monitor Overview" on page 408.
  - "UNIX Resources Monitor Overview" on page 654.

Note: Make sure to select **Enable Server-Centric Report** and select the required measurements. For details on the measurements, see "Server-Centric Report Measurements" on page 1333.

- For details on creating a monitor using solution templates (this is recommended because the templates contain all the required measurement counters), see:
  - "Microsoft Windows Host Solution Template" on page 1207
  - "AIX Host Solution Template" on page 1113
  - "Linux Host Solution Template" on page 1157
  - "Solaris Host Solution Templates" on page 1253

2 Generate the Server-Centric report

To monitor your server, navigate to the SiteScope Dashboard, display the data for the applicable Microsoft Windows or UNIX Resources monitor, and click the server name in the **Target** column in the row that corresponds to your resources monitor. The Server-Centric report opens.

3 Analyze data in the report

The report enables you to view three different metrics of your server in the same graph – CPU utilization, memory utilization, and network utilization. It also lists the top five processes by CPU utilization and memory consumption. You can drill down to specific times by clicking a data point on the graph.

For user interface details, see "Server-Centric Report" on page 1334.

How to Create a Server-Centric Report – Use-Case Scenario

This use-case scenario describes how to create a Server-Centric report.

Note: For a task related to this scenario, see "How to Create a Server-Centric Report" on page 1326.

This scenario includes the following steps:

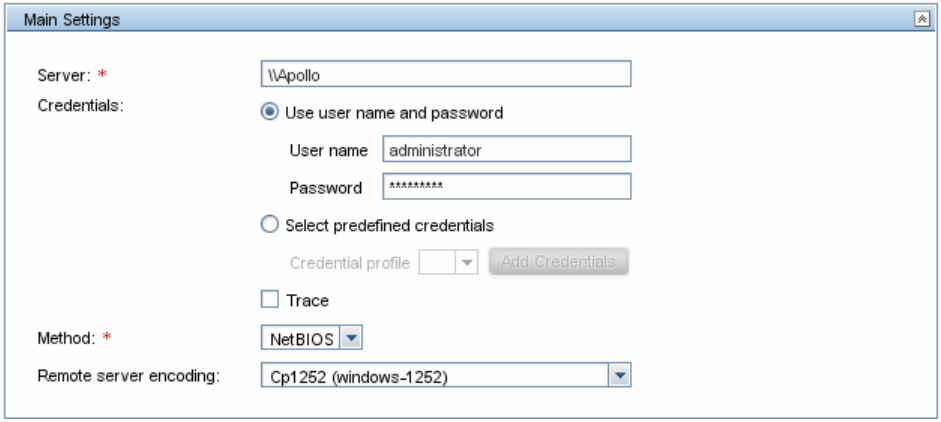
- "Background" on page 1329
- "Configuring a remote server" on page 1329
- "Deploying a Microsoft Windows Host solution template" on page 1330
- "Creating a Server-Centric report" on page 1331

1 Background

David Foster, a SiteScope user at NewSoft Company, wants to create a report that provides data on CPU utilization, memory utilization, and network utilization for a monitored server, Apollo.

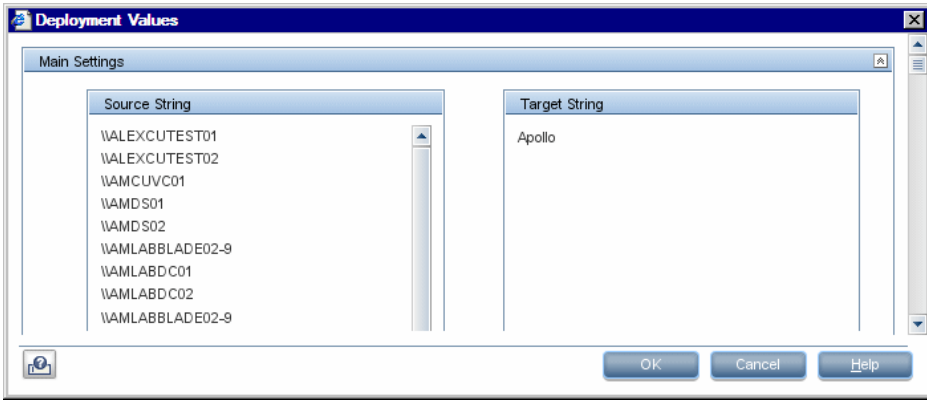
2 Configuring a remote server

Before he creates the report, David configures SiteScope to monitor the remote Windows server, Apollo, and configures the server in Microsoft Windows Remote Servers.

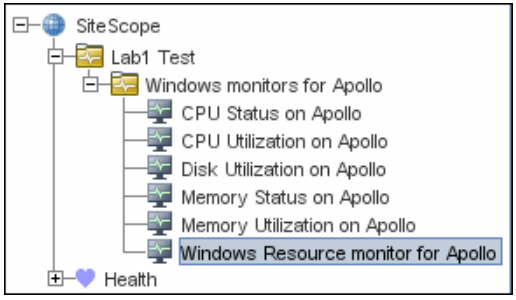


3 Deploying a Microsoft Windows Host solution template

After enabling SiteScope to monitor data on Apollo, David deploys the Microsoft Windows Host solution template into the selected group container, and selects Apollo as the server to monitor. David uses the solution templates when creating the Microsoft Windows Resource monitor, because the required monitors and metrics for generating a Server-Centric report are already configured.

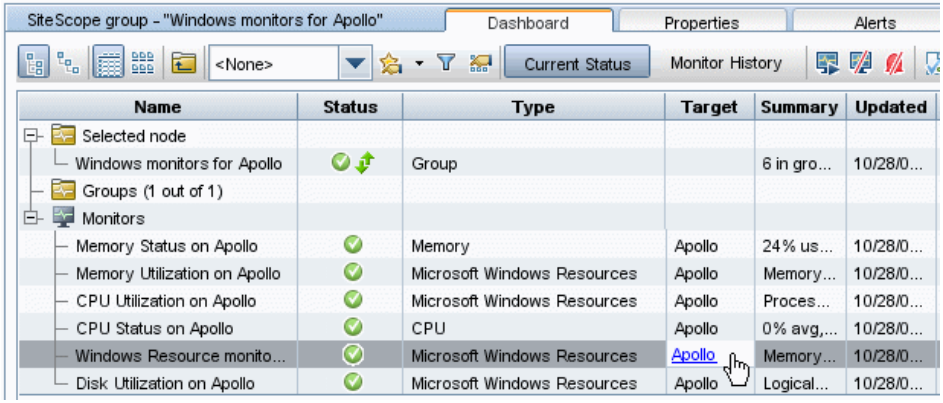


After David deploys the solution template, SiteScope creates a group named Windows monitors for Apollo that contains the Microsoft Windows Resources monitor.

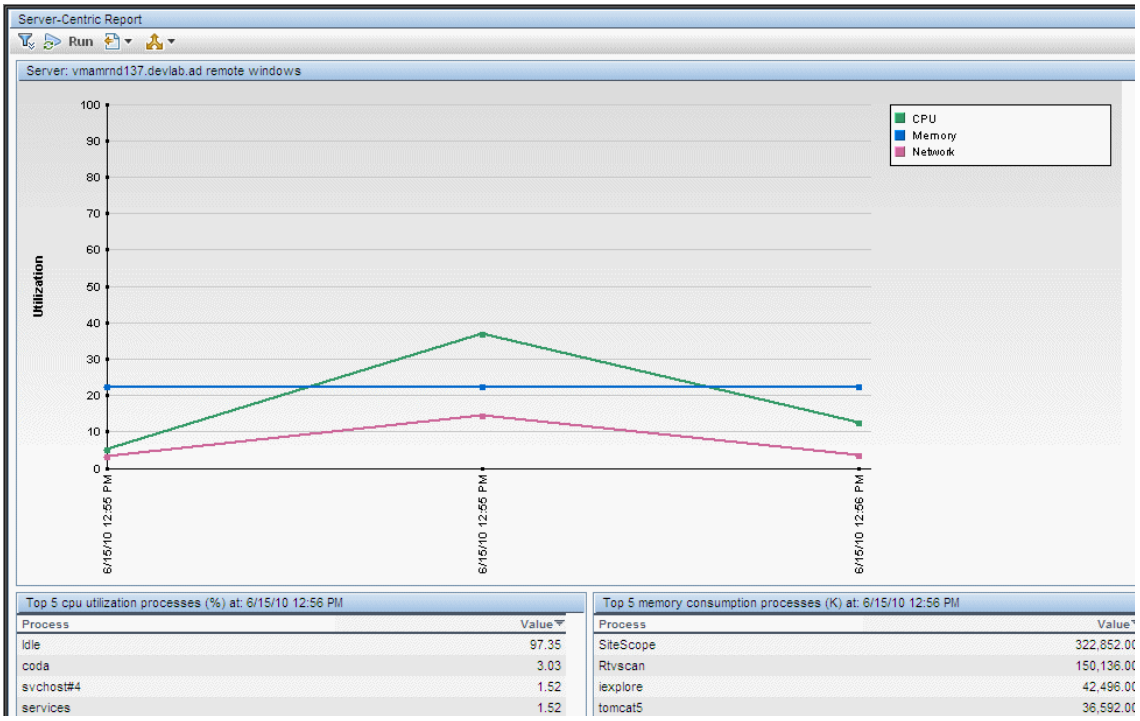


4 Creating a Server-Centric report

David generates the Server-Centric report for Apollo from the Current Status view of Service Health.



The Server-Centric report opens, displaying the CPU Utilization, Memory Utilization, and Network Utilization metrics on the same graph. David can use this data to view the top processes by CPU utilization and memory consumption during different times, and focus in on problematic periods to locate the processes running at that time.



Reference

Server-Centric Report Measurements

The following table displays the counters which must be selected when defining the monitor for the Server-Centric report manually:

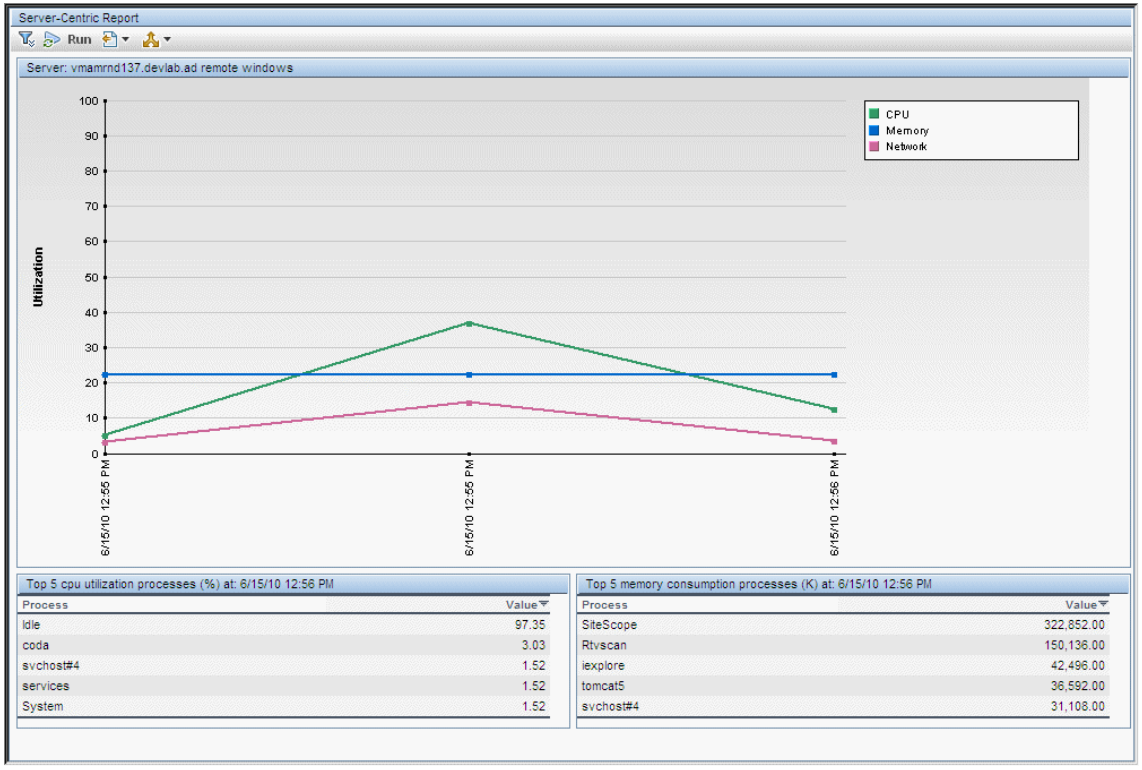
OS Type	Server-Centric Mandatory Counters
Counters for Microsoft Windows Resource Monitor	Memory\% Committed Bytes In Use
	Processor_Total\% Processor Time
Counters for UNIX Resource Monitor on Solaris Platform	CPU utilization\%sys
	CPU utilization\%usr
	CPU utilization\%wio
	Memory\swap_avail
	Memory\swap_resv
Counters for UNIX Resource Monitor on AIX Platform	Processor\Total\%sys
	Processor\Total\%usr
	Processor\Total\%wio
Counters for UNIX Resource Monitor on Linux Platform	Memory\MemFree
	Memory\MemTotal
	Processor\Total\System
	Processor\Total\User
	Processor\Total\User low

For details on selecting counters for monitor definition, see:

- "Microsoft Windows Resources Monitor Settings" on page 416 (for Microsoft Windows Resources monitor counters).
- "UNIX Resources Monitor Settings" on page 657 (for Solaris, AIX, and Linux platforms).

Server-Centric Report

This report displays the metrics CPU utilization, memory utilization, and network utilization for a selected server.



To access	Select the **Monitors** context. Click the server name link in the **Target** column of SiteScope Dashboard for a Microsoft Windows Resources or UNIX Resources monitor.
Important information	➤ This report is available only on those servers being monitored by a dedicated Microsoft Windows Resources monitor or UNIX Resources monitor created for the purpose of running the report. ➤ We highly recommend that you deploy these monitors using the applicable solution templates for these monitors. The templates are preconfigured with the correct measurement counters and options already selected. ➤ The Server-Centric report is not supported in Firefox 2.x. ➤ 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.
Relevant tasks	"How to Create a Server-Centric Report" on page 1326
See also	➤ "Generating a Server-Centric Report" on page 1324 ➤ "How to Create a Server-Centric Report – Use-Case Scenario" on page 1328

Report Settings

User interface elements are described below:

UI Element	Description
	**Format.** Formats the report data to a file for exporting. Select the format for the file. The options are printer-friendly, CSV, Excel, or XML.
	**Export.** Exports the report data in an email. Select the option for sending the file. The options are HTML mail, HTML attachment, or PDF. **Note:** To use the export functionality, you must add the SiteScope machine to the trusted sites.
	**Filter/Collapse report filter.** Click to display/hide the time range settings for the report.
	**Back.** Displays the report one time frame earlier than the currently displayed time frame. **Example:** If the value of the **View** box is **Day**, clicking this button displays data for one day earlier than the currently displayed report.
	**Forward.** Displays the report one time frame later than the currently displayed time frame. **Example:** If the value of the **View** box is **Day**, clicking this button displays data for one day later than the currently displayed report.
View	Time range for which you want to view the report. Available time ranges include the following: ➤ Custom (enables you to configure any range) ➤ Hour, Day, Week ➤ Past hour, Past day, Past week

UI Element	Description
From/To <date links>	Click the **From** link to configure a start date and time for the report. Click the **To** link to configure an end date and time for the report. The calendar contains the following buttons: ➤ **OK.** Updates the date link for the selected date and closes the calendar. ➤ **Revert.** Returns to the previously selected report date. ➤ **Current.** Selects today's date in the calendar. ➤ **Cancel.** Closes the calendar without making any changes.
	Creates a report for the date range displayed in the date links (Filter).

Report Content

User interface elements are described below:

UI 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	Name of the server appears above the Utilization graph.
Utilization graph	Displays 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.
Top 5 CPU Utilization Processes table	Displays 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	Displays 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.

67

SiteScope Server Health

This chapter includes:

Concepts

Tasks

Reference

Concepts

SiteScope Health Overview

SiteScope Health is a specially designed group of monitors that display information about the performance and availability of SiteScope itself. Health monitors retrieve data about SiteScope's resource usage, key processes, monitor load, server parameters, and the integrity of key configuration files.

By default, the daily monitor logs record the SiteScope Health monitoring data and let you can create reports on SiteScope's performance and operational health. These log files are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions. For example, SiteScope's audit log contains configuration changes performed in the new user interface, such as creation of monitors, templates, alerts, and so forth.

Together with the SiteScope Health monitoring, the SiteScope Progress Report provides several key indicators you use to monitor the performance of the SiteScope application.

This section also includes:

➤ "Skipped Monitor Events" on page 1341

➤ "Problems Reporting Data" on page 1342

Skipped Monitor Events

A SiteScope monitor is reported as skipped if the monitor fails to complete its actions before it is scheduled to run again. This can occur with monitors that have complex actions to perform, such as querying databases, stepping through multi-page URL sequences, waiting for scripts to run, or waiting for an application that has hung.

For example, assume you have a URL Sequence Monitor that is configured to transit a series of eight Web pages. This sequence includes performing a search which may have a slow response time. The monitor is set to run once every 60 seconds. When the system is responding well, the monitor can run to completion in 45 seconds. However, at times, the search request takes longer and then it takes up to 90 seconds to complete the transaction. In this case, the monitor has not completed before SiteScope is scheduled to run the monitor again. SiteScope detects this and makes a log event in the SiteScope **skip_monitor.log**. The SiteScope Log Event Monitor detects this and signals an error status. For log file details, see "Log File Types" on page 1410.

A monitor may also skip if it is a monitor type that requires a process from the process pool but the process pool limit has been reached. Generally, this is not likely to happen but may occur in some situations with high monitoring load. The SiteScope Health Log Event Monitor also watches for process pool events. Skipped monitors can cause loss of data when a monitor run is suspended due because a previous run has not completed or has become hung by a unresponsive application. They can also cause SiteScope to automatically stop and restart itself, an event that is also monitored by the SiteScope Health Log Event Monitor. A restart is done in an effort to clear problems and reset monitors. However, this can also lead to gaps in monitoring coverage and data. Adjusting the run frequency at which a monitor is set to run or specifying an applicable timeout value can often correct the problem of skipping monitors.

Note:

- You can enable a setting that automatically disables monitors that exceed the maximum allowed skip count. If this occurs, SiteScope shuts down with an error and sends an email to the SiteScope administrator about the skipping monitor to signal the disable event. To enable this setting: In the preferences view, click **Infrastructure Preferences**, and expand the **Skip Monitor Settings** pane. Select the **Shutdown on monitor skips** check box. You can also determine the time period that a monitor is disabled. For details on skipped monitor settings, see "Skip Monitor Settings" on page 729.
- You can control the maximum number of processes available. You should only change this setting if adjustments to monitor configurations do not resolve the monitor performance problems. The initial value is 200 processes per pool (by default, the maximum processes per pool is 20). To change this setting: In the preferences view, click **Infrastructure Preferences**, and expand the **General Settings** pane. Configure the number of processes in the **Maximum processes per pool** box.

Problems Reporting Data

SiteScope Health monitors are also configured to report events that indicate a problem with the transfer of SiteScope monitor and configuration data to a BSM installation. For information about troubleshooting data reporting to BSM, see "Troubleshooting and Limitations" on page 304.

SiteScope Health Group

SiteScope Health monitors can monitor several key aspects of its own environment to help uncover monitor configuration problems as well as SiteScope server load. SiteScope can also monitor its connectivity and related data events when connected to BSM.

Similar to regular monitors, Health monitors can be edited to reconfigure their frequency and thresholds. Administrators can enhance the Health group by adding new monitors targeting additional servers and environments.

The Health monitor group is displayed as a health icon within the main SiteScope container. You view the contents of the Health monitor group by clicking the **Health** container.

SiteScope Health monitoring includes the following monitor types:

Monitor Type	Default Name	Description
BAC Integration Configuration Monitor	BSM Integration Configuration	Checks the correctness of the configuration between SiteScope and BSM when SiteScope is configured as a data collector for BSM.
BAC Integration Statistics Monitor	BSM Integration Statistics	Checks the traffic volume between SiteScope and BSM when SiteScope is configured as a data collector for BSM.
Connection Statistics Monitor	Connection Statistics Monitor	Checks the status of SSH and Telnet connections when used to connect to remote UNIX or Windows servers. Also checks Perfex and Perfex dispatcher statistics and statuses for each perfex pool.
Dynamic Monitoring Statistics	Dynamic Monitoring Statistics	Checks performance of the dynamic monitoring framework when you have dynamic monitors defined.

Monitor Type	Default Name	Description
SiteScope Server Health Monitor	Health of SiteScope Server	Checks a large number of server process and resources for the server on which SiteScope is running.
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.
SSL Certificates State Monitor	SSL Certificates State	Checks the state of SSL certificates in the default keystore.

BAC Integration Configuration Monitor

When SiteScope is integrated as a data collector for BSM, this health monitor enables you to track the correctness of SiteScope's integration with the BSM configuration. This monitor is useful for viewing the number of groups, monitors, and measurements reporting to BSM that have an invalid path, internal name, or ID. It also displays the number of duplicate Topaz IDs, and instances where the Topaz ID is (-1).

For details on configuring the monitor, see "BAC Integration Configuration Monitor Page" on page 1352.

Troubleshooting and Limitations

This section describes troubleshooting and limitations when working with SiteScope Server Health.

- If there are objects with duplicate BSM IDs or with BSM ID == (-1):
  - Open a JMX Console (there is one provided in **<SiteScope root directory>\java\bin\jconsole.exe**), and enter 28006 in the **Port** field.
  - In the **MBeans** tab, select **com.mercury.sitescope/Integration/Bac/Tools/BacIntegrationToolsJMX**.
    - For objects with duplicate BSM IDs, activate fixDuplicateBACConfiguration().
    - For objects with BSM ID == (-1), activate fixMinusOneBACConfiguration().
  - It is also recommended to activate softSync() to send the new configuration to BSM.
- If measurements have the wrong category ID, you should restart SiteScope.

BAC Integration Statistics Monitor

The BAC Integration Statistics monitor checks the health of BSM. When SiteScope is integrated as a data collector for BSM, this health monitor enables you to track the volume of traffic between SiteScope and BSM. SiteScope sends metrics to BSM every minutes. For details on configuring the monitor, see "BAC Integration Statistics Monitor Page" on page 1354.

Connection Statistics Monitor

The Connection Statistics monitor provides an overview of global connection handles. It collects data on SSH and Telnet connection behavior, and statistics for the Perfex and Perfex_dispatcher pool. This monitor is useful for analyzing connection problems and remote server configuration issues. For details on configuring the monitor, see "Connection Statistics Monitor Page" on page 1355.

Dynamic Monitoring Statistics

The Dynamic Monitoring Statistics monitor provides an overview of the performance of the dynamic monitoring framework when you have dynamic monitors defined. It is useful for viewing performance and for analyzing problems when using the dynamic monitoring mechanism to automatically update dynamic monitoring counters and thresholds. For details on configuring the monitor, see "Dynamic Monitoring Statistics Page" on page 1359.

SiteScope Server Health Monitor

The Health of SiteScope Server Monitor is the equivalent of a SiteScope monitor that monitors server resources on the server where SiteScope is running. This includes monitors for CPU, disk space, memory, and key processes. A problem with resource usage on the SiteScope server may be caused by monitors with configuration problems or may simply indicate that a particular SiteScope is reaching 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. For details on SiteScope data logging options, see "Log Preferences" on page 783. For details on configuring the monitor, see "Health of SiteScope Server Monitor Page" on page 1362.

SiteScope Log Events Monitor

The Log Event Monitor is the equivalent of a SiteScope monitor group that writes errors to the SiteScope Error Log (**error.log**) for certain events. These events include Log entries indicating that a monitor has been skipped or there was a problem in reporting data to another application. For details on configuring the monitor, see "Log Event Health Monitor Page" on page 1366.

SiteScope Monitor Load Monitor

The Monitor Load Monitor watches how many monitors are running and how many are waiting to be run. Watching monitor load is important to help maintain monitoring performance and continuity. If the number of monitors waiting approaches or exceeds the number of monitors running, adjustments should be made to monitor configurations to reduce the number of monitors waiting to run. Generally, this can be done by reducing the run frequency of some monitors. For details on configuring the monitor, see "Monitor Load Monitor Page" on page 1369.

Tasks

How to Analyze SiteScope Health Monitor Data

This task describes the steps involved in analyzing SiteScope Health monitor data and viewing the SiteScope log files and server statistics.

This task includes the following steps:

- "Prerequisites" on page 1348
- "Deploy SiteScope Health monitors" on page 1349
- "View SiteScope Health monitors" on page 1349
- "View SiteScope log files" on page 1350
- "View monitor performance data" on page 1350

1 Prerequisites

To access the log files and the Progress Report, you must have the correct user privileges.

a In the left pane, click **Preferences** and select **User Management Preferences**.

b Right-click the user name, and select **Edit User**.

c In the Edit User Profile dialog box, expand **Permissions.**

d In the **Other** section, make sure that **View server statistics** and **View logs** are selected (these settings are selected by default).

2 Deploy SiteScope Health monitors

If the SiteScope Health monitors are not present when you import a SiteScope to System Availability Management in BSM, you must deploy the monitors.

For task details, see "Deploy SiteScope Health Monitors" on page 1351.

Note: The SiteScope health monitors are normally present, because they are enabled automatically when SiteScope is deployed.

---

3 View SiteScope Health monitors

You can view the data collected by the SiteScope Health monitors in the SiteScope Dashboard.

For user interface details, see "SiteScope Health User Interface" on page 1352.

Example:

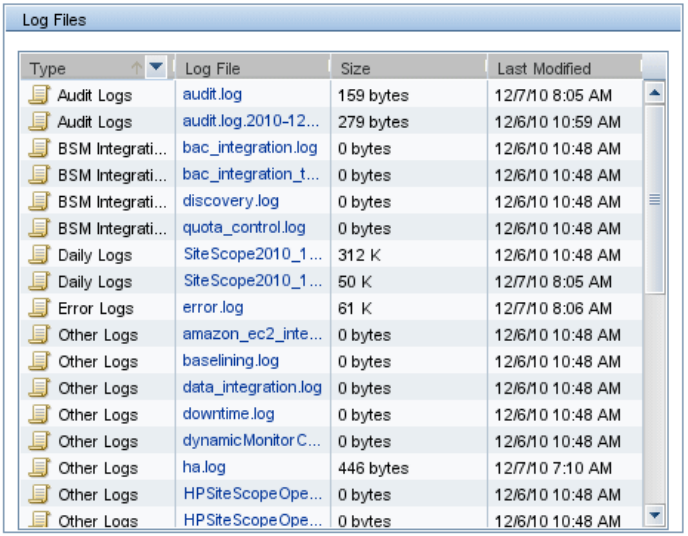
Name	Status	Type	Target	Summary	Updated	Description
Selected node						
Health		Group		8 in group,1...	2/1/11 3:5...	
Groups (0 out of 0)						
Monitors (8 out of 8)						
BAC Integration Configuration		BACIntegr...		Total Grou...	2/1/11 3:2...	
BAC Integration Statistics		BAC Integ...		Currently lo...	2/1/11 3:5...	
Connection Statistics Monitor		Connectio...		SSH conne...	2/1/11 3:5...	
Dynamic Monitoring Statistics		DynamicM...		Average ta...	2/1/11 3:5...	
Health of SiteScope Server		Monitor Lo...	SiteScop...	{ Threshold...	2/1/11 3:5...	
Log Event Checker		Log Event ...		.*skipped #...	2/1/11 3:5...	
Monitor Load Checker		Monitor Lo...		Current Mo...	2/1/11 3:5...	
SSL Certificates State		SSLCertifi...		Expired cer...	2/1/11 3:2...	

4 View SiteScope log files

You can view the various SiteScope log files in the Log Files page in the Server Statistics context.

For user interface details, see "Log Files Page" on page 1409.

Example:



5 View monitor performance data

You can view the load on the SiteScope server and a list of the most recently run monitors in the Server Statistics context.

For concept details, see "Using Server Statistics" on page 1372.

Deploy SiteScope Health Monitors

This task describes how to deploy SiteScope Health monitors to a SiteScope installation if the monitors were not present when you imported a SiteScope to System Availability Management in BSM.

Note: This task is part of a higher-level task. For details, see "How to Analyze SiteScope Health Monitor Data" on page 1348.

To deploy SiteScope Health monitors to a SiteScope installation:

1 Open the SiteScope container to which you want to display the Health monitors. Confirm that the SiteScope includes the Health monitor group container.

Note: The Health monitor group container is identified with a health indicator icon.

---

2 Find the **Health Templates** in the monitor tree. Click to expand the container contents. The available Health monitor templates are displayed.

3 Select the Health monitor template for the operating system on which the SiteScope you want to monitor is running. The choices are:

- UNIX Health Monitors
- Windows Health Monitors

4 Right-click the template icon and select **Copy** from the action menu.

5 Right-click the **Health** monitor group container of the SiteScope to which you want to deploy the Health monitors and select **Paste**. The monitors in the selected template are then configured and deployed to the selected SiteScope server.

Reference

SiteScope Health User Interface

This section includes:

BAC Integration Configuration Monitor Page

This page enables you to check the correctness of SiteScope's integration with the BSM configuration.

To access	Select the **Monitors** context. In the monitor tree, expand **Health** and click **BAC Integration Configuration**.
Important information	Monitor data is relevant only if SiteScope is integrated as a data collector for BSM.
See also	➤ "BAC Integration Configuration Monitor" on page 1345 ➤ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 447.

Main Settings

User interface elements are described below:

UI Element	Description
Counters	➤ **Total Groups.** Total number of groups reporting data to BSM. ➤ **Total Monitors.** Total number of monitors reporting data to BSM. ➤ **Duplicate BSM ID.** Number of duplicate BSM IDs reported to BSM. Every SiteScope object has a unique BSM ID. If two objects have the same ID, only one of these objects can send its data to BSM. For troubleshooting on this subject, see "Troubleshooting and Limitations" on page 1345. ➤ **BSM ID == (-1).** Every SiteScope object has a unique BSM ID. If the ID value for a SiteScope object is (-1), SiteScope does not send its data to BSM. For troubleshooting on this subject, see "Troubleshooting and Limitations" on page 1345. ➤ **Group with invalid path.** If the SiteScope group does not have a valid path, SiteScope does not send the group to BSM. ➤ **Groups with duplicate name.** If the SiteScope group does not have a unique internal name, SiteScope does not send the group to BSM. ➤ **Monitor with invalid path.** If the SiteScope monitor does not have a valid path, SiteScope does not send the monitor to BSM. ➤ **Monitors without internal ID.** If the SiteScope monitor does not contain a unique internal ID, SiteScope does not send the monitor to BSM. ➤ **Monitors without internal name.** If the SiteScope monitor does not contain a valid internal name, SiteScope does not send this monitor to BSM. ➤ **Measurements with wrong category ID.** If SiteScope measurements do not contain a valid category ID, SiteScope does not send the measurements to BSM. For troubleshooting on this subject, see "Troubleshooting and Limitations" on page 1345. ➤ **Target with BSM ID == (-1).** Every remote target has a unique BSM ID. If the ID value is (-1), SiteScope does not send its data to BSM. For troubleshooting on this subject, see "Troubleshooting and Limitations" on page 1345.

BAC Integration Statistics Monitor Page

This page enables you to check the volume of traffic between SiteScope and BSM.

To access	Select the **Monitors** context. In the monitor tree, expand **Health** and click **BAC Integration Statistics**.
Important information	Monitor data is relevant only if SiteScope is integrated as a data collector for BSM.
See also	➤ "BAC Integration Statistics Monitor" on page 1346 ➤ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 447.

Main Settings

User interface elements are described below:

UI Element	Description
Counters	➤ **Currently Logging to Business Service Management.** Displays the amount of metrics currently logging per minute to BSM. ➤ **Number of Topology Scripts in Queue.** Displays the number of topology scripts waiting to be run. These scripts forward topology data to BSM and must be run whenever there is a configuration change in SiteScope. The queue can grow when a SiteScope is first registered to BSM or when there are many configuration changes made in the SiteScope.

Connection Statistics Monitor Page

This page provides an overview of global connection handles. It collects data on SSH and Telnet connection behavior, and statistics for the Perfex and Perfex_dispatcher pool. This monitor is useful for analyzing connection problems and remote server configuration issues.

To access	Select the **Monitors** context. In the monitor tree, expand **Health** and click **Connection Statistics Monitor**.
See also	➤ "Connection Statistics Monitor" on page 1346 ➤ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 447.

Main Settings

User interface elements are described below:

UI Element	Description
SSH Connection Counters	➤ **Total opened.** Total number of all opened SSH connections. If this number is significantly higher than the **Currently allocated resources** counter, this indicates a configuration problem. You should check the following: ➤ Connection cache was disabled ➤ An incorrect login or password was used ➤ The remote server timeout is too short ➤ **Total closed.** The number of SSH connections closed since the last SiteScope restart. ➤ **Total failed to open V1.** The number of SSH connections that failed to open using SSH version 1. By default, SiteScope tries to connect using V1 before trying to connect with V2. If this number is high, we recommend selecting the **SSH version 2 only** option on the problematic remote server. ➤ **Total failed to open V2.** The number of SSH connections that failed to open using SSH version 2. If this number is high, you should verify the correct login and password was used for the remote server, and verify the SSH version on the remote server (V1 or V2). ➤ **Reused.** The number of reused SSH connections since the last SiteScope restart. ➤ **Currently allocated resources.** The number of SSH connections that are currently open. ➤ **Currently in use.** The number of SSH connections that are currently open and in use running monitors.

UI Element	Description
Telnet Connection Counters	➤ **Total opened.** The number of telnet connections opened since the last SiteScope restart. ➤ **Total closed.** The number of telnet connections closed since the last SiteScope restart. ➤ **Reused.** The number of reused telnet connections since the last SiteScope restart. ➤ **Currently allocated resources.** The number of telnet connections that are currently open. ➤ **Currently in use.** The number of telnet connections that are currently open and in use running monitors.

UI Element	Description
Perfex/Perfex dispatcher Connection Counters	➤ **Idle processes.** The number of processes currently in idle state. ➤ **Used processes.** The number of processes currently in used state. ➤ **Total processes.** The total number of processes (idle processes + used processes). ➤ **Process pool queue length.** The number of monitors currently waiting for an available perfex. This value can indicate that there are too many monitors running on perfex, or that the perfex pool is too small. ➤ **Average wait time for free process.** The average amount of time to wait, in milliseconds, for a process to be available. If this value exceeds 30,000 milliseconds (30 seconds), monitors will start to fail. A high average wait time indicates that you need to increase the number of processes in the pool. ➤ **Average run time.** The average amount of time, in milliseconds, that a perfex takes to run. This gives an indication of the following: ➤ Network speed. The amount of time it takes to send a request and receive a response from the server. ➤ Perfex availability. How long it takes on average to complete the run and to return the perfex to the pool. ➤ The number of monitors using perfex. ➤ **Processes waiting for server timeout**. The number of processes that have exceeded the call timeout and are waiting for a server timeout to close the connection, or that are waiting for an answer to return to the pool.

Dynamic Monitoring Statistics Page

This page displays statistics when using the dynamic monitoring mechanism to automatically update dynamic monitoring counters and thresholds. It shows the total number of times a specific dynamic monitoring action occurred, and the number of occurrences during the last 10 minutes. This monitor is useful for viewing performance and for analyzing problems in dynamic monitoring.

To access	Select the **Monitors** context. In the monitor tree, expand **Health** and click **Dynamic Monitoring Statistics**.
Important information	This information is also available from the **Server Statistics** context by clicking the **Dynamic Monitoring** tab.
See also	➤ "Dynamic Monitoring Statistics" on page 1346 ➤ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 447.

Main Settings

User interface elements are described below:

UI Element	Description
Counters	
Average task run time (milliseconds)	Average amount of time, in milliseconds, it took for a task to run.
Average task run time during last 10 minutes (milliseconds)	Average amount of time, in milliseconds, it took for a task to run during the last 10 minutes.
Average task wait time (milliseconds)	Average amount of time, in milliseconds, it took for a task to start running since the time it was received.

UI Element	Description
Average task wait time during last 10 minutes (milliseconds)	Average amount of time, in milliseconds, it took for a task to start running since the time it was received, during the last 10 minutes.
Number of clashes between dynamic monitoring framework and concurrent user changes during last 10 minutes	Number of times unable to save dynamic monitoring framework changes as a result of the user making concurrent changes (so as not to override user changes), during the last 10 minutes.
Number of times the maximum number of matching counters was exceeded during last 10 minutes	Number of times that the matching counters (for patterns) from the server exceeded the limit during the last 10 minutes.
Number of times there were no matching counters from server during last 10 minutes	Number of times there were no matching counters for patterns from the server during the last 10 minutes.
Number of times unable to extract counters from file during last 10 minutes	Number of times unable to extract counters from the counters file during the last 10 minutes.
Number of times unable to retrieve counters from server during last 10 minutes	Number of times unable to retrieve counters from the server during the last 10 minutes.

UI Element	Description
Number of times unable to run dynamic tasks because of resource exhaustion during last 10 minutes	Number of times unable to run dynamic tasks because the maximum dynamic monitoring framework thread pool and queue size limits were reached, during the last 10 minutes. You can configure these settings in **Preferences > Infrastructure Preferences > Dynamic Monitoring Settings**. For details, see "Dynamic Monitoring Settings" on page 730.
Number of times unable to save changes during last 10 minutes	Number of times unable to save counter changes to SiteScope persistency during the last 10 minutes.
Number of unsaved counter files during last 10 minutes	Number of times unable to delete existing counter files or save new counter files during the last 10 minutes.

Health of SiteScope Server Monitor Page

This page enables you to check the SiteScope server resource and process statistics for the local SiteScope installation.

To access	Select the **Monitors** context. In the monitor tree, expand **Health** and click **Health of SiteScope Server**.
Important information	➤ Process/perfex counters were removed from the SiteScope Server Health monitor and are no longer supported. ➤ **Note when working in template mode:** The maximum number of counters that you can select is 100. If you import a template monitor from an earlier version of SiteScope, or perform a copy to template action, the number of counters is not limited.
Relevant tasks	"How to Analyze SiteScope Health Monitor Data" on page 1348
See also	➤ "SiteScope Server Health Monitor" on page 1347 ➤ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 447.

Health of SiteScope Server Monitor Settings

User interface elements are described below:

UI Element	Description
Counters (on UNIX)	➤ Current Monitors Run Per Minute ➤ Current Monitors Running ➤ Current Monitors Waiting ➤ Maximum Monitors Run Per Minute ➤ Maximum Monitors Running ➤ Maximum Monitors Waiting ➤ Used Disk Space on SiteScope Drive (accessible on SiteScope installed on UNIX) ➤ MegaBytes Available on SiteScope Drive ➤ 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

UI Element	Description
Counters (on Windows)	**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

UI Element	Description
Counters (on Windows)	**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

UI Element	Description
Counters (on Windows)	**Server** ➤ Bytes Total/sec ➤ Errors Logon ➤ Errors Access Permissions ➤ Errors System ➤ Files Open ➤ Server Sessions

Log Event Health Monitor Page

This page enables you to monitor the local SiteScope installation **error.log** file for certain events. These events include log entries indicating that a monitor has been skipped or there was a problem in reporting data to another application.

To access	Select the **Monitors** context. In the monitor tree, expand **Health** and click **Log Event Checker**.
Relevant tasks	"How to Analyze SiteScope Health Monitor Data" on page 1348
See also	➤ "SiteScope Log Events Monitor" on page 1347 ➤ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 447.

Log Event Health Monitor Settings

User interface elements are described below:

UI Element	Description
Counters	➤ **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 is 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 BSM. ➤ **Error. config reporter failed to report chunk of data.** There was a fault in the transfer of SiteScope configuration data to System Availability Management in BSM. ➤ **Error. HP Business Service Management failed to process data.** BSM reported a fault in processing data sent from SiteScope.

UI Element	Description
Counters	➤ **Error. CacheSender. Got to the max number of cached files.** SiteScope has reached the maximum number of cached data file awaiting transfer to BSM. This may occur if data transfer between SiteScope and BSM has been interrupted. ➤ **Error. CacheSender. Got to the max old dir size.** SiteScope has reached the maximum directory size for cached data file awaiting transfer to BSM. This may occur if data transfer between SiteScope and BSM has been interrupted. ➤ **HP Business Service Management SEVERE.** BSM reported a data transfer or processing fault with a status of SEVERE. ➤ **Commit verification failed.** ➤ **Error loading monitor.** ➤ **Error contacting mirror server.** ➤ **Error: open SSH connections limit reached.** ➤ **Error: failure in baseline process.** ➤ **Error: failed to parse rule.** ➤ **Topology Reporter failed to report.**
Reset counter values	Resets the monitor counter values to 0.

Monitor Load Monitor Page

This page enables you to check several SiteScope load statistics reported by the Progress Report for the local SiteScope installation.

To access	Select the **Monitors** context. In the monitor tree, expand **Health** and click **Monitor Load Checker**.
Relevant tasks	"How to Analyze SiteScope Health Monitor Data" on page 1348
See also	➤ "SiteScope Monitor Load Monitor" on page 1347 ➤ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 447.

Monitor Load Monitor Settings

User interface elements are described below:

UI Element	Description
Counters	➤ Current Monitors Run Per Minute ➤ Current Monitors Running ➤ Current Monitors Waiting ➤ Maximum Monitors Run Per Minute ➤ Maximum Monitors Running ➤ Maximum Monitors Waiting

SSL Certificates State Monitor Page

This page enables you to check the state of SSL certificates in the default keystore (**<SiteScope root directory>\java\lib\security\cacerts**). This is where client certificates that are imported for monitoring URL, WebSphere Application Server, or VMware-based servers are stored.

To access	Select the **Monitors** context. In the monitor tree, expand **Health** and click **SSL Certificates State**.
Relevant tasks	"How to Analyze SiteScope Health Monitor Data" on page 1348
See also	➤ "Certificate Management" on page 907 ➤ The monitor specific settings are described below. For details on the settings common to all monitors, see "Common Monitor Settings" on page 447.

SSL Certificates State Monitor Settings

User interface elements are described below:

UI Element	Description
Days before expiration	If a certificate is due to expire within the specified number of days (but has not yet expired), it is added to the **Certificates expiring soon** counter. **Default value:** 7 days
Counters	➤ Expired certificates. Comma-separated list of already expired certificates ➤ Certificates expiring soon. Comma-separated list of certificates that are due to expire within the period specified in Days before expiration. soon (fasted that N days, determined by monitor settings), but not expired yet. ➤ Number of expired certificates ➤ Number of certificates expiring soon

68

Viewing Server Statistics

This chapter includes:

Concepts

Tasks

Reference

Concepts

Using Server Statistics

The SiteScope **Server Statistics** context provides an overview of several key SiteScope server performance metrics that can be used for analyzing SiteScope performance, stability, health, and for debugging bottlenecks. It includes statistics that show load on the SiteScope server, a list of running monitors and the most recently run monitors, perfex pool summary, WMI statistics, SSH connections, Telnet connections, and dynamic monitoring statistics. It also displays the SiteScope log files. The Server Statistics context is updated every 20 seconds.

The Server Statistics context includes the following pages:

Page	Description
General	Displays key SiteScope server load statistics, including the number of monitors running and waiting, and a list of running monitors by type. For details of the user interface, see "General Page" on page 1393.
Running Monitors	Displays a list of which SiteScope monitors are running, and which monitors have run recently, at what time, and what was the returned status. For details of the user interface, see "Running Monitors Page" on page 1394.
Perfex Process Pool	Displays a process manager summary, and statistics tables for the perfex and perfex_dispatcher pools. For details of the user interface, see "Perfex Process Pool Page" on page 1396.
WMI Statistics	Displays the process manager summary for Windows Management Instrumentation (WMI) statistics. For details of the user interface, see "WMI Statistics Page" on page 1399.

Page	Description
SSH Connections	Displays SSH statistics and SSH connection summary when using SSH to connect to remote UNIX or Windows servers. For details of the user interface, see "SSH Connections Page" on page 1401.
Telnet Connections	Displays telnet statistics when using telnet to connect to remote UNIX or Windows servers. For details of the user interface, see "Telnet Connections Page" on page 1403.
Dynamic Monitoring	Displays statistics when using the dynamic monitoring mechanism to automatically update counters and thresholds for dynamic monitors. For details of the user interface, see "Dynamic Monitoring Page" on page 1405.
Log Files	Displays the list of log files in SiteScope that are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions. For details of the user interface, see "Log Files Page" on page 1409.

Interpreting SiteScope Server Load Statistics

Monitoring Load can be a key indicator of SiteScope scaling problems, monitor configuration problems, or network performance issues. The following is a brief explanation of the SiteScope monitor execution model and interpreting the server performance data in the context of this model.

A SiteScope monitor instance is essential as an instruction set that is run by the SiteScope application on a regularly scheduled interval. While a monitor instance is defined, SiteScope queues the monitor for execution based on the run (update) frequency and schedule options. If the monitor instance is marked as disabled, it is still scheduled in the queue but the normal instructions are not run.

As a Java-based application, SiteScope makes use of multi-threading to accomplish parallel execution of monitor tasks. Each monitor instance scheduled for execution is assigned a thread. Once it is assigned a thread, the monitor instance becomes a **Monitor Running**. It remains bound to the thread until the monitor execution instruction has either received a result or the timeout value, if applicable, has been reached.

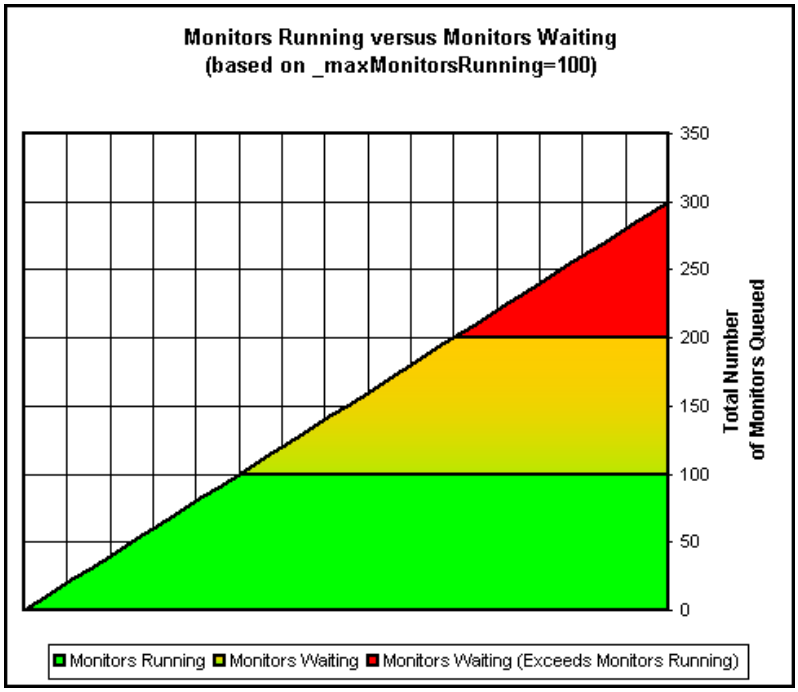
Even in this model, monitor execution is not instantaneous and there is a finite limit to the number of monitor threads that can be run in parallel. If not more threads are available, a monitor that is queued for execution becomes a **Monitor Waiting** for an execution thread.

It is difficult to assign specific values and limits to SiteScope Monitoring Load because the specifics of the server capacity and network deployment can vary widely. The monitoring load may also vary significantly over time simply due to transient network traffic issues or SiteScope monitor configuration problems.

One key warning signal for interpreting monitoring load is the ratio of Monitors Waiting to Monitors Running. Generally, having some monitors waiting for execution is not a problem unless the ratio of Monitors Waiting to Monitors Running is consistently 1:2 or higher. For example, if the number of monitors running is at the maximum of 100 and there are 50 monitors waiting, this represents a ratio of 1 monitor waiting for every two running.

Note: The initial maximum number of monitor execution threads for the _maxMonitorsRunning= setting controlled by the **master.config** file is 400 (the default value is 30 in **master.xml**).

The graph below presents a visualization of the relationship between Monitors Running and Monitors Waiting. This graph is based on the _maxMonitorsRunning setting of 100 monitors. The green region shows that SiteScope can run all queued monitors until the number of queued monitors exceeds 100. At that level, additional monitors that are scheduled to run are given the status of Monitor Waiting. The red region represents an area where the number of monitors waiting is more than twice the number of monitors running. This is a certain indication that your SiteScope monitor configurations are not well aligned with the capacity of the server and network.



You can adjust the following monitor configuration settings if there are consistently too many monitors waiting:

- **Frequency.** This is the basic schedule parameter for every monitor type. A large number of Monitors Running and Monitors Waiting can often be explained by a large number of monitors set to run (or update) at short intervals. The minimum update interval is 15 seconds. Depending on a number of system factors, there are several monitor actions which may take more than 15 seconds to complete. For example, Web transactions, database queries, logging onto remote servers, and some regular expression matches may delay monitor completion. Use the "Monitor Summary Report" on page 1546 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 1546 to list monitors that may have the **Verify error** setting enabled.

For details on SiteScope server performance data, see "Running Monitors Page" on page 1394.

Using Log Files

SiteScope maintains a number of log files that are useful for understanding SiteScope performance issues, for troubleshooting monitor and alert problems, and for reviewing SiteScope management actions.

Log files can be accessed using the Log File menu in the Server Statistics context. When you click a log file, a new browser window opens displaying the text of the log file. You can use the scroll bars to view the contents of the log or use the browser's text Find utility to locate specific information. For example, you can search for a unique text string that appears in a monitor's **Name** property to locate entries for a particular monitor instance. For details on the various SiteScope log files, see "Log Files Page" on page 1409.

The log files are written in plain text and stored in the **<SiteScope_root_path>\logs** directory. In the default configuration, these log files are tab-delimited text files. Understanding the order and content of these files is useful for examining particular monitor results or for porting the SiteScope monitor results to another database. For details, see "SiteScope Log File Columns" on page 1381.

Note: SiteScope log files do not support Unicode characters—all non-English characters appear corrupted in the logs. As a workaround, use a SiteScope server installed on a corresponding operating system locale. For example, use SiteScope installed on a Japanese Windows operating system for a Japanese locale.

This section also includes:

Using the Audit Log

SiteScope's audit log provides you with a record of actions performed in SiteScope, the time they were performed, and by whom. It contains configuration changes performed in the new user interface, such as creation of monitors, templates, alerts, and so forth.

Note: When SiteScope is attached to SAM Admin in HP Business Service Management, the actions you perform on SiteScope appear in HP Business Service Management's audit log and not in SiteScope's audit log.

As each operation is performed, an entry is made in the audit log. When the current audit log reaches its size limit, it is closed and a new log is created. Older logs are named audit.log.1, audit.log.2, and so forth. The higher the number concatenated to the name, the older the log. For details on setting the size limit and the maximum number of backup audit logs to be kept, see "How to Configure the Audit Log" on page 1380.

The name of the current audit log is **audit.log** and it is found in the **<SiteScope root directory>\logs** directory. You can access the audit log from the directory or through the SiteScope application. For details on viewing the audit log, see "Log Files Page" on page 1409.

Most operations performed in the monitor tree are recorded in the audit log. For a list of operations that are not recorded in the audit log, see "Audit Log Limitations" on page 1378.

Audit Log Limitations

- Audit log entries can be created only in English. This means that audit log entries are also displayed only in English, regardless of what language you use to view SiteScope.
- The following operations are not recorded in the audit log:
  - When a template is deployed, operations on the various elements in the template are not logged.

    For example, you deployed a template that created group MM2_Servers with monitors in the new group. The audit log entry is:

    Operation performed: Configuration Template 'MM2' pasted on ‘MM2_Servers’.

    Note that there are no entries in the audit log about creation of monitors in MM2_Servers group.
  - Attaching and detaching SiteScope to HP Business Service Management are not logged.

    When SiteScope is attached to SAM Admin in BSM, the actions you perform on SiteScope appear in HP Business Service Management’s audit log and not in SiteScope’s audit log.

Tasks

How to Analyze SiteScope Server Statistics

This task describes the steps involved in analyzing SiteScope server statistics and log files.

This task includes the following steps:

- "Prerequisites" on page 1379
- "View SiteScope server statistics" on page 1379
- "View SiteScope log files" on page 1379

1 Prerequisites

To access the Server Statistics context, you must be an administrator in SiteScope, or a user granted **View server statistics** permissions (this settings is selected by default).

For details on user permissions, see "Permissions" on page 873.

2 View SiteScope server statistics

You can view the load on the SiteScope server, a list of running and most recently run monitors, perfex process pool, WMI, SSH connections, telnet connections, and dynamic monitoring statistics in the Server Statistics context.

For user interface details, see "SiteScope Server Statistics User Interface" on page 1392.

3 View SiteScope log files

You can view the various SiteScope log files in the Log Files page in the Server Statistics context.

For user interface details, see "Log Files Page" on page 1409.

How to Configure the Audit Log

This task describes the steps involved in configuring the maximum size of the audit log.

1. Open the **log4j.properties** file located in the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** directory.
2. Set **MaxFileSize** to the maximum number of lines in the log.
3. Set **MaxBackupIndex** to the maximum number of backup audit logs to be kept before the oldest audit log is deleted.

   For example, if **MaxBackupIndex** is 5, no more than 5 backup audit logs are kept. If 5 backup log files exist, then after the current audit.log file reaches **MaxFileSize** size, audit.log.5 is deleted, audit.log.4 is renamed to audit.log.5, audit.log.3 to audit.log.4 and so forth. The current audit.log is renamed audit.log.1 and a new audit.log is created.

Reference

SiteScope Log File Columns

When SiteScope runs a monitor instruction to test the availability of components in the infrastructure, the monitor results are written to data log files. The first six columns of each log entry in a SiteScope monitor data log are the same for each monitor type. After the first six columns of each log entry, the content of each column is specific for each monitor type.

The following table describes the content of these columns. The columns in each log file are written as tab-delimited text.

Column	Data in Column
1	Time and date the sample was recorded.
2	Category (for example, good, error, warning, nodata).
3	Monitor group name where the monitor defined (also called ownerID).
4	Monitor title text.
5	stateString (this is the status string that shows up on the Group details page).
6	id:sample number (a unique ID for this monitor where group + id is a unique key for a monitor). The sample number is a unique sample number for that monitor.

Audit Log Entries

Each line of the audit log describes an operation performed in SiteScope.

This section includes:

SiteScope Startup

When SiteScope is restarted, its entry is:

```
YYYY-MM-DD HH:MM:SS - SiteScope Audit Log initialized
```

Group Operations

Operations performed on groups have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Group
'<group_name>' '<operation>' '<container>'
```

where:

- **<group_name>** is the name of the group that was operated on.
- **<operation>** can be one of the following:
  - **Created In.** The location where the group was created.
  - **Updated in.** The location where the group's information was updated.
  - **Deleted From.** The location from where the group was deleted.
  - **Pasted On.** The user copied information from one group to another.
- **<container>** is the name of the group container that was operated on.

Monitor Operations

Operations performed on monitors have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Monitor
‘<monitor_name>’ ‘<operation>’ ’<container>’
```

- <**monitor_name**> is the name of the monitor that was operated on.
- <**operation**> can be one of the following:
  - **Created In.** The location where the user created a monitor.
  - **Updated in.** The location from where the user updated a monitor’s information.
  - **Deleted From.** The location where the user deleted a monitor.
  - **Pasted On.** The user copied information from one monitor to another.
- <**container**> is the name of the container.

Update to General Preferences

Changes made in **General Preferences** under the **Preferences** container in the monitor tree have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed:
‘<preferences_name>’ updated
```

where <**preferences_name**> is the name of the preference that was changed.

The nature of the change to the preference is not in the log.

Update to Other Preferences

Changes to preferences other than those listed in **General Preferences** in the monitor tree have the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed:
‘<preferences_name>’ named ‘<object_name>’ ‘<operation>’
```

- <**preferences_name**> is the name of the preference.
- <**object_name**> is the name of the object to which the preference refers.
- <**operation**> can be one of the following:
  - **Updated.** The user changed the preference.
  - **Deleted.** The user deleted the preference.

This format is used for the following types of preferences:

- Microsoft Windows Remote Servers
- UNIX Remote Servers
- Mail Preferences
- Pager Preferences
- SNMP Preferences
- Absolute Schedule Preferences
- Range Schedule Preferences
- User Management Preferences

Applying Templates

When an entity is created by deploying a template, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Configuration
Template '<template_name>' pasted on '<group_name>'
```

- <**template_name**> is the name of the template from which the entity was created.
- <**group_name**> is the name of the group that contains the entity that was created from the template.

Note: To see which entities were created by deploying the template, look at the contents of template itself. Information about entities is not included in the audit log.

Template Containers

When a template container is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
Container '<container_name>' '<operation>' '<container>'
```

- <**container_name**> is the name of the template container that was either created, deleted, or updated.
- <**operation**> can be one of the following:
  - **Created in.** The location where the user created the template container.
  - **Deleted from.** The location from where the user deleted the template container.
  - **Updated in.** The location where the user changed the template container.
- <**container**> is the name of the container containing the template.

Create, Delete, Modify Templates

When a template is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
'<template_name>' '<operation>' '<container>'
```

- **<template_name>** is the name of the template that was either created, deleted, or updated.
- **<operation>** can be one of the following:
  - **Created in.** The location where the user created the template.
  - **Deleted from.** The location from where the user deleted the template.
  - **Updated in.** The location where the user changed the template.
- **<container>** is the name of the container containing the template.

Template Variables

When a template variable related to an object, such as server ID, is created, deleted, or updated in a container, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
Variable '<variable_name>' '<operation>' '<container>'
```

- **<variable_name>** is the name of the variable that was either created, deleted, or updated.
- **<operation>** can be one of the following:
  - **Created in.** The location where the template variable for the object was created.
  - **Deleted from.** The location where the template variable for the object was deleted.
  - **Updated in.** The location where the template variable for the object was updated.
- **<container>** is the name of the container containing the template variable.

Template Groups

When a template group for a specific type of object is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template Group
'<group_name>' '<operation>' '<container>'
```

- <**group_name**> is the name of the template group created, updated or deleted.
- <**operation**> can be one of the following:
  - **Created in.** The location where the template group for the object was created.
  - **Deleted from.** The location from where the template group for the object was deleted.
  - **Updated in.** The location where template for the object was updated.
- <**container**> is the name of the container containing the template group.

Template Remote Objects

When a template remote server is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
Remote '<remote_name>' '<operation>' '<container>'
```

- <**remote_name**> is the name of the remote server.
- <**operation**> can be one of the following:
  - **Created in.** The location where the remote entity was created.
  - **Deleted from.** The location from where the remote entity was deleted.
  - **Updated in.** The location where the remote entity was updated.
- <**container**> is the name of the container containing the remote entity.

Template Alerts

When a template for an alert is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template Alert
'<alert_name>' '<operation>' '<container>'
```

- <**alert_name**> is the name of the object for which the template alert is defined.
- <**operation**> can be one of the following:
  - **Created in.** The location where the template alert was created.
  - **Deleted from.** The location from where the template alert was deleted.
  - **Updated in.** The location where the template alert was updated.
- <**container**> is the name of the template container.

Template Monitors

When a template for a monitor is created, deleted, or updated, the log entry is:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Template
'<monitor_name>' '<operation>' '<container>'
```

- <**monitor_name**> is the name of the monitor.
- <**operation**> can be one of the following:
  - **Created in.** The location where the template for the monitor was created.
  - **Deleted from.** The location from where the template for the monitor was deleted.
  - **Updated in.** The location where the template for the monitor was updated.
- <**container**> is the name of the container containing the template.

Alerts

Operations performed on alerts are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Alert
'<alert_name>' '<operation>' '<container>'
```

- <**alert_name**> is the name of the alert.
- <**operation**> can be one of the following:
  - **Created In.** The location where the new alert was created.
  - **Updated in.** The location where the new alert was updated.
  - **Deleted From.** The location from where the new alert was deleted.
  - **Pasted On.** The user copied information from one alert to another.
- <**container** > is the container of the alert.

Reports

Operations performed on report definitions are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Report
'<report_name>' '<operation>' '<container>'
```

- <**report_name**> is the name of the report.
- <**operation**> can be one of the following:
  - **Created In.** The location where a new report was created.
  - **Updated in.** The location where a new report was updated.
  - **Deleted From.** The location from where a new report was deleted.
  - **Pasted On.** The information was copied from one report to another.
- <**container** >**.** The container of the report.

Global Search and Replace Operations

Global Search and Replace operations are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: GSAR operation started
---------------------------------------------------------------------------------------------
YYYY-MM-DD HH:MM:SS -Global Replace updated group '<group_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated report '<report_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated monitor '<monitor_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated alert '<alert_name>'
YYYY-MM-DD HH:MM:SS -Global Replace updated preference '<preference_name>'
---------------------------------------------------------------------------------------------
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: GSAR operation finished
```

Start and end operations always appear in the log. The entries appear depending on the actions performed by the Global Search and Replace.

Login-Logout

Login and logout are in the format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: <message>
```

where <**message**> is either:

- Logged in.
- Logged out.

Failed Login

Failed login attempts are in the format:

```
YYYY-MM-DD HH:MM:SS - Username and password do not match. Failed to login.
```

Changed Password

Password operations are logged and appear in the following format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: <message>
```

where <**message**> is either:

- Changed password successfully.
- Failed to change password.

Categories

Operations performed on categories are logged and appear in the following format:

```
YYYY-MM-DD HH:MM:SS - User: <username> Operation Performed: Category
'<category_name>' '<operation>'
```

- <**category_name**> is the name of the category.
- <**operation**> can be one of the following:
  - **Created.** The location where a new category was created.
  - **Updated.** The location where a new category was updated.
  - **Deleted.** The location from where a new category was deleted.

SiteScope Server Statistics User Interface

This section includes:

➤ Telnet Connections Page on page 1403

➤ Dynamic Monitoring Page on page 1405

➤ Log Files Page on page 1409

General Page

This page enables you to view an overview of several key SiteScope server performance statistics, including the current and maximum number of running monitors, waiting monitors, and monitor runs per minute. It also displays a list of monitor types that are currently running, and the number of running instances for each type.

To access	Select **Server Statistics** context > **General**
Important information	Only an administrator in SiteScope, or a user granted **View server statistics** permissions, can view the monitor performance data pages. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Analyze SiteScope Server Statistics" on page 1379
See also	"Using Server Statistics" on page 1372

User interface elements are described below:

UI Element	Description
Overall Statistics	
Monitors running	**Current** column. Displays the number of monitors queued for execution, based on their update frequency or schedule, that currently have execution threads. This means they are being run. **Maximum** and **Measured on** columns. Display the maximum number of monitors that ran and when they ran.

UI Element	Description
Monitors waiting	**Current** column. Displays the number of monitors queued for execution, based on their update frequency or schedule, that currently are awaiting execution threads. This means they are not being run. **Maximum** and **Measured on** columns. Display the maximum number of monitors that were waiting at any one time and when this occurred.
Monitors run per minute	**Current** column. Displays a rolling average of the last 10 minutes of monitoring, and tracks the rate (per minute) at which monitors are being run. **Maximum** and **Measured on** columns. Display the maximum number of monitors running per minute at any one time and when they ran.
Running Monitors by Type	
<running monitors list>	Displays a list of monitor types that are currently running and the number of running instances for each type.

Running Monitors Page

This page enables you to view a list of which SiteScope monitors are running, and which monitors have run recently, at what time, and what was the returned status.

To access	Select **Server Statistics** context > **Running Monitors**
Important information	Only an administrator, or a user granted **View server statistics** permissions, can view the monitor performance data pages. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Analyze SiteScope Server Statistics" on page 1379
See also	"Using Server Statistics" on page 1372

User interface elements are described below:

UI Element	Description
Running Monitors	
Run Time	The run time, in seconds, for the monitor that is currently being run.
Skips	The number of skips for the monitor that is currently being run. A SiteScope monitor is reported as skipped if it fails to complete its actions before it is scheduled to run again.
Group Name	The group to which the monitor that is currently being run belong.
Monitor Name	The name of the SiteScope monitor that is currently being run. Clicking the monitor name link opens the Dashboard page for the selected monitor. Monitors with longer run time or skips are colored in red.
Current Status	The status returned by the monitor that is currently being run. For example,
Recent Monitor Runs	
Time and Date	The date and time the monitor ran. The monitors are displayed in the order that have most recently completed running.
Group Name	The group to which the monitor belongs.
Monitor Name	The name of the monitor that SiteScope ran.
Current Status	The status returned by the monitor (**good**, **warning**, **error**) and measurement summary details.

Perfex Process Pool Page

This page displays the process manager summary, and pool statistics and statuses for each perfex pool. Perfex is a command line interface to processor event counters. Perfex prints the values of various hardware performance counters after the given command is complete. Perfex_dispatcher is a process used for Microsoft Windows Resources monitors.

To access	Select **Server Statistics** context > **Perfex Process Pool**
Important information	Only an administrator, or a user granted **View server statistics** permissions, can view the monitor performance data pages. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Analyze SiteScope Server Statistics" on page 1379
See also	"Using Server Statistics" on page 1372

User interface elements are described below:

UI Element	Description
Process Manager Summary	
Calls per minute	The number of process calls on the Sitescope server, per minute.
Double failures	The number of times SiteScope failed to connect to a remote server, after making two consecutive connection attempts. For connection failure details, check the run monitor and error logs.
Stopped processes	The number of processes that stopped due to error, for example, if the process timed out, since the last SiteScope restart.
Created processes	The number of processes created by SiteScope for all pools since the last restart. If there is a large number of created processes and stopped processes, you should increase the perfex timeout value in **Preferences** > **Infrastructure Preferences** > **General Settings** > **Perfex timeout (seconds)**.

UI Element	Description
Cleaned processes	SiteScope cleans processes if they exceed the maximum idle time. The default time before cleaning idle processes is 10 minutes. You can change the idle processes maximum time in **Preferences** > **Infrastructure Preferences** > **General Settings** > **Maximum idle time for perfex process in minutes**. Cleaning processes improves the memory footprint on the SiteScope machine. Cleaning processes is especially important during a network slowdown when perfexes take longer to finish. As a result, more perfexes are created, but they are not used.
Pool Statistics - perfex/perfex_dispatcher	
Process pool queue length	The number of monitors currently waiting for an available perfex. This value can indicate that there are too many monitors running on perfex, or that the perfex pool is too small.
Average wait time for free process (milliseconds)	The average amount of time to wait, in milliseconds, for a process to be available. If this value exceeds 30,000 milliseconds (30 seconds), monitors will start to fail. A high average wait time indicates that you need to increase the number of processes in the pool.
Average run time (milliseconds)	The average amount of time, in milliseconds, that a perfex takes to run. This gives an indication of the following: ➤ Network speed. The amount of time it takes to send a request and receive a response from the server. ➤ Perfex availability. How long it takes on average to complete the run and to return the perfex to the pool. ➤ The number of monitors using perfex.
Idle processes	The number of processes currently in idle state.
Used processes	The number of processes currently in used state.

UI Element	Description
Total processes	The total number of processes (idle processes + used processes).
Maximum process pool size	The maximum number of processes allowed per process pool. The default value is 200. You can change the maximum process pool size in **Infrastructure Preferences** > **General Settings** > **Maximum processes per pool**.
Processes waiting for server timeout	The number of processes that have exceeded the call timeout and are waiting for a server timeout to close the connection, or that are waiting for an answer to return to the pool.

WMI Statistics Page

This page displays the process manager summary for Windows Management Instrumentation (WMI) statistics. You can use WMI to access system counter data from objects in the performance libraries. This is the same performance data that appears in the Perfmon utility.

To access	Select **Server Statistics** context > **WMI Statistics**
Important information	Only an administrator, or a user granted **View server statistics** permissions, can view the monitor performance data pages. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Analyze SiteScope Server Statistics" on page 1379
See also	"Using Server Statistics" on page 1372

User interface elements are described below:

UI Element	Description
Process Manager Summary	
Calls per minute	The number of process calls on the Sitescope server, per minute.
Double failures	The number of times SiteScope failed to connect to a remote server, after making two consecutive connection attempts. For connection failure details, check the run monitor and error logs.
Stopped processes	The number of processes that stopped due to error, for example, if the process timed out, since the last SiteScope restart.

UI Element	Description
Created processes	The number of processes created by SiteScope for all pools since the last restart. If there is a large number of created processes and stopped processes, you should increase the perfex timeout value in **Preferences** > **Infrastructure Preferences** > **General Settings** > **Perfex timeout (seconds)**.
Cleaned processes	SiteScope cleans processes if they exceed the maximum idle time. The default time before cleaning idle processes is 10 minutes. You can change the idle processes maximum time in **Preferences** > **Infrastructure Preferences** > **General Settings** > **Maximum idle time for perfex process in minutes**. Cleaning processes improves the memory footprint on the SiteScope machine. Cleaning processes is especially important during a network slowdown when perfexes take longer to finish. As a result, more perfexes are created, but they are not used.
Processes waiting for server timeout	The number of processes that have exceeded the call timeout and are waiting for a server timeout to close the connection, or that are waiting for an answer to return to the pool.

SSH Connections Page

This page displays Secure Shell (SSH) statistics and a summary of SSH connections when using SSH to connect to remote UNIX or Windows servers.

To access	Select **Server Statistics** context > **SSH Connections**
Important information	Only an administrator, or a user granted **View server statistics** permissions, can view the monitor performance data pages. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Analyze SiteScope Server Statistics" on page 1379
See also	"Using Server Statistics" on page 1372

User interface elements are described below:

UI Element	Description
SSH Statistics	
Total opened	Total number of all opened SSH connections. If this number is significantly higher than the **Currently allocated resources** counter, this indicates a configuration problem. You should check the following: ➤ Connection cache was disabled ➤ An incorrect login or password was used ➤ The remote server timeout is too short
Total closed	The number of SSH connections closed since the last SiteScope restart.
Total failed to open V1	The number of SSH connections that failed to open using SSH version 1. By default, SiteScope tries to connect using V1 before trying to connect with V2. If this number is high, we recommend selecting the **SSH version 2 only** option on the problematic remote server.

UI Element	Description
Total failed to open V2	The number of SSH connections that failed to open using SSH version 2. If this number is high, you should verify the correct login and password was used for the remote server, and verify the SSH version on the remote server (V1 or V2).
Reused	The number of reused SSH connections since the last SiteScope restart.
Currently allocated resources	The number of SSH connections that are currently open.
Currently in use	The number of SSH connections that are currently open and in use running monitors.
SSH Connections Summary	
<Host name>	For each target remote server, there is a row that displays the following information: ➤ **Machine Name.** The name of the monitored remote server. ➤ **Sessions in Use.** The number of open SSH sessions on the monitored remote server. ➤ **Idle Sessions.** The number of idle SSH sessions on the monitored remote server. ➤ **Maximum Sessions.** The maximum number of SSH sessions (idle or in use) on the monitored remote server. ➤ **Queue Length.** The number of SSH sessions in the queue. ➤ **Average Wait Time.** The average amount of time to wait, in milliseconds, for a free SSH session. **Note:** SiteScope has a limit of 500 concurrent SSH connections.

Telnet Connections Page

This page displays telnet statistics when using telnet to connect to remote UNIX or Windows servers.

To access	Select **Server Statistics** context > **Telnet Connections**
Important information	Only an administrator, or a user granted **View server statistics** permissions, can view the monitor performance data pages. For details on user permissions, see "User Management Preferences Overview" on page 846.
Relevant tasks	"How to Analyze SiteScope Server Statistics" on page 1379
See also	"Using Server Statistics" on page 1372

User interface elements are described below:

Parameter	Description
Telnet Statistics	
Total opened	The number of telnet connections opened since the last SiteScope restart.
Total closed	The number of telnet connections closed since the last SiteScope restart.
Reused	The number of reused telnet connections since the last SiteScope restart.
Currently allocated resources	The number of telnet connections that are currently open.

Parameter	Description
Currently in use	The number of telnet connections that are currently open and in use running monitors.
Telnet Connections Summary	
<Host name>	For each target remote server, there is a row that displays the following information: ➤ **Machine Name.** The name of the monitored remote server. ➤ **Sessions in Use.** The number of open telnet sessions on the monitored remote server. ➤ **Idle Sessions.** The number of idle telnet sessions on the monitored remote server. ➤ **Maximum Sessions.** The maximum number of telnet sessions (idle or in use) on the monitored remote server. ➤ **Queue Length.** The number of telnet sessions in the queue. ➤ **Average Wait Time.** The average amount of time to wait, in milliseconds, for a free telnet session. **Note:** SiteScope has a limit of 500 concurrent telnet connections.

Dynamic Monitoring Page

This page displays statistics when using the dynamic monitoring mechanism to automatically update dynamic monitoring counters and thresholds. This is useful for viewing performance and for analyzing problems in dynamic monitoring.

To access	Select **Server Statistics** context > **Dynamic Monitoring**
Important information	➤ Only an administrator, or a user granted **View server statistics** permissions, can view the monitor performance data pages. For details on user permissions, see "User Management Preferences Overview" on page 846. ➤ This information is also available from the **Monitors** context (expand the **Health** folder and click **Dynamic Monitoring Statistics**).
Relevant tasks	"How to Analyze SiteScope Server Statistics" on page 1379
See also	"Using Server Statistics" on page 1372

User interface elements are described below:

Parameter	Description
Average task wait time during last 10 minutes (milliseconds)	Average amount of time, in milliseconds, it took for a task to start running since the time it was received, during the last 10 minutes.
Average task wait time (milliseconds)	Average amount of time, in milliseconds, it took for a task to start running since the time it was received.
Average task run time during last 10 minutes (milliseconds)	Average amount of time, in milliseconds, it took for a task to run during the last 10 minutes.
Average task run time (milliseconds)	Average amount of time, in milliseconds, it took for a task to run.

Parameter	Description
Number of unsaved counter files during last 10 minutes	Number of times unable to delete existing counter files or save new counter files during the last 10 minutes.
Number of clashes between dynamic monitoring framework and concurrent user changes during last 10 minutes	Number of times unable to save dynamic monitoring framework changes as a result of the user making concurrent changes (so as not to override user changes), during the last 10 minutes.
Number of times the maximum number of matching counters was exceeded during last 10 minutes	Number of times that the matching counters (for patterns) from the server exceeded the limit during the last 10 minutes.
Number of times unable to extract counters from file during last 10 minutes	Number of times unable to extract counters from the counters file during the last 10 minutes.
Number of times unable to save changes during last 10 minutes	Number of times unable to save counter changes to SiteScope persistency during the last 10 minutes.
Number of times unable to run dynamic tasks because of resource exhaustion during last 10 minutes	Number of times unable to run dynamic tasks because the maximum dynamic monitoring framework thread pool and queue size limits were reached, during the last 10 minutes. You can configure these settings in **Preferences** > **Infrastructure Preferences** > **Dynamic Monitoring Settings**. For details, see "Dynamic Monitoring Settings" on page 730.

Parameter	Description
Number of times unable to retrieve counters from server during last 10 minutes	Number of times unable to retrieve counters from the server during the last 10 minutes.
Number of times there were no matching counters from server during last 10 minutes	Number of times there were no matching counters (for patterns) from the server during the last 10 minutes.
Total number of unsaved counter files	Total number of times unable to delete existing counter files or save new counter files.
Total number of clashes between dynamic monitoring framework and concurrent user changes	Total number of times unable to save dynamic monitoring framework changes as a result of the user making concurrent changes (so as not to override user changes).
Total number of times the maximum number of matching counters was exceeded	Number of times that the matching counters (for patterns) from the server exceeded the limit.
Total number of times unable to extract counters from file	Total number of times unable to extract counters from the counters file.
Total number of times unable to save changes	Total number of times unable to save counter changes to SiteScope persistency.

Parameter	Description
Total number of times unable to run dynamic tasks because of resource exhaustion	Total number of times unable to run dynamic tasks because the maximum dynamic monitoring framework thread pool and queue sizes limits were reached. You can configure these settings in **Preferences** > **Infrastructure Preferences** > **Dynamic Monitoring Settings**. For details, see "Dynamic Monitoring Settings" on page 730.
Total number of times unable to retrieve counters from server	Total number of times unable to retrieve counters from the server.
Total number of times there were no matching counters from server	Total number of times there were no matching counters (for patterns) from the server.

Log Files Page

This page enables you to inspect the SiteScope log files.

To access	Select **Server Statistics** context > **Log Files**.
Important information	SiteScope log files do not support Unicode characters—all non-English characters appear corrupted in the logs. As a workaround, use a SiteScope server installed on a corresponding operating system locale. For example, use SiteScope installed on a Japanese Windows operating system for a Japanese locale.
Relevant tasks	➤ "How to Analyze SiteScope Server Statistics" on page 1379 ➤ "How to Configure the Audit Log" on page 1380
See also	➤ "Using Log Files" on page 1376 ➤ "SiteScope Log File Columns" on page 1381 ➤ "Audit Log Entries" on page 1382 ➤ "Audit Log Limitations" on page 1378

Log Files Table

User interface elements are described below:

UI Element	Description
	Changes the sort order in the columns by clicking the arrow in the column title. A small up or down arrow is displayed to the left of the arrow which indicates the sort order. **Note:** Clicking the arrow in the **Type** column title opens the list of log types, which enables you to filter the list by the log type you want to display. To clear the filter, click the arrow again, and select **(All)**.
Type	The log file type. For details on the different types of log files, see "Log File Types" on page 1410.
Log File	The name of the log file. Double-click a log file link to open the file in your Web browser.

UI Element	Description
Size	The size of the log file.
Last Modified	The time and date on which the log file was last modified.

Log File Types

User interface elements are described below:

UI Element	Description
Audit Logs	Contains links to the logs containing all configuration changes that were performed, such as creation of monitors, templates, alerts and so on. For details on audit logs, see "Using the Audit Log" on page 1377.
BSM Integration Logs	Contains information about connectivity and monitor data transfer when SiteScope is configured to report to BSM.
Daily Logs	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.
Error Logs	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 Logs	Contains information about specific monitor runs and actions related to managing monitors. This can be useful in troubleshooting monitors.

UI Element	Description
Other Logs Contains various different log file types, such as:	
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.
monitorCount.log	Counts the total number of monitors and license points used in SiteScope. It also specifies the number and license point usage for each type of server health monitor. This log is updated once a day when SiteScope starts (and not on every change). You can refresh the log file at any time by selecting **Help** > **About SiteScope**.
Operator.log	An optional log file used to record SiteScope operator actions, primarily information from use of the Acknowledgement function. This log is created when an acknowledgement is added to one or more monitors.
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.
remotes_multi_test	Displays the remote server connection test results when the test was performed for multiple remotes.
silent_deployment	Records details on submitted requests for silent deployments and their corresponding deployment results. It also includes error messages for silent deployments that fail. This log is updated once a day when SiteScope starts (and not on every change). **Note:** When deploying a template using a CSV file, non-English characters used in the CSV file are not supported in the silent_deployment log file. The deployment values are displayed correctly in the user interface if the correct encoding option is selected.

UI Element	Description
skip_monitor.log	Records details on skipped monitors. For every skip occurrence, a line is added with the date and time of the skip, name (and ID) of the monitor, server name, number of skips, and the monitor status (if the monitor was disabled).
URL Details log	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.

Part XI

Alerts and Reports

69

SiteScope Alerts

This chapter includes:

Concepts

Tasks

Reference

- SiteScope Alert Templates Directory on page 1450
- SiteScope Alert Template and Event Properties Directory on page 1451
- SiteScope Alerts User Interface on page 1461

Concepts

SiteScope Alerts Overview

SiteScope alerts are notification actions that are triggered when the conditions for the alert definition are detected. You use an alert to send some notification of an event or change of status in some element or system in your infrastructure. For example, an alert can be triggered when a SiteScope monitor detects a change from Good to Error indicating that the monitored system has stopped responding.

An alert definition contains settings that tell SiteScope what monitors can trigger the alert, what condition to watch for, what information to send, and who should be the recipients of the alert. For example, you can create an alert that includes instructions for SiteScope to send the specific server address and error code to your pager or email when an error condition is detected on a particular system. You can also have SiteScope respond to problems by automatically initiating recovery or action scripts with Script Alert. For example, you can configure a Script Alert to run a script to restart a server if a monitor detects that a system is no longer responding and CPU utilization has reached 100%. For details on the alert types, see "Action Type Dialog Box" on page 1473.

SiteScope alerts can be configured in several ways. Alerts can be associated with one or more individual monitors, with one or more groups of monitors, a combination of monitors and groups, or globally for all monitors and groups. Global and group-wide alerting is generally the most efficient but may not provide the needed control.

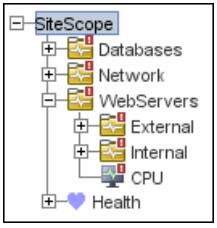
You can use the **Filter Settings** function on each alert definition page to create filter criteria to control global and group alerts to more specific criteria. Filter criteria can be used to restrict the alert to only monitors of a certain type, that contain a certain text string, tag, or other filter criteria. For example, creating a global alert with a filter criteria for CPU Monitor creates an alert that is triggered only for the CPU monitor type. You can also control individual monitor alerts using tags. For example, you can create an individual monitor alert with a filter criteria for selected tags that is triggered only if the monitor contains one of these tags. If you set up a global or root alert and assign tags to it, and assign the same tags to a group, an alert is not triggered for this group of monitors if none of the monitors in the group contain the same tags as in the alert.

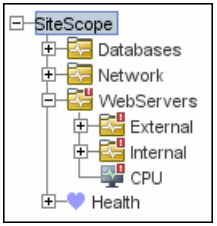
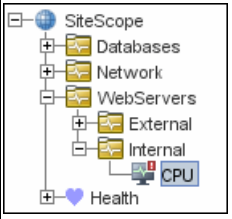
For details on how to configure alerts, see "SiteScope Alerts Page" on page 1461.

Note: You can also use the SiteScope API when working with alerts. For details, see "Using the SiteScope Configuration API" on page 42.

Alert Associations and Considerations

The table below displays an overview of the different alert 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.  **Note**: We do not recommend creating 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 an 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.  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 required. However, you should plan and consolidate alerts to keep the number of alert definitions to a minimum. This facilitates alert administration and helps reduce redundant alert messages or actions.

Creating Alert Actions

When you create an alert scheme in SiteScope, you create alert actions to be triggered when the alert conditions are met. You create alert actions using the Alert Action dialog box. While in the dialog box, you determine the following:

- The type of alert action. For a detailed list of available alert actions, see "Action Type Dialog Box" on page 1473.
- The settings for the type of alert being sent. For example, you can define the recipients and their addresses for an email alert action.
- The status condition that triggers the alert. For example, you can instruct SiteScope to trigger an alert action when a monitor's status changes to error or unavailable.
- The trigger settings that determine when the alert is triggered and when it is sent. For details, see "Understanding When SiteScope Alerts Are Sent" on page 1422.

You can create multiple alert actions for an alert scheme.

- **Multiple methods of delivery**. You can create an alert action to send a sound alert and another alert action to send an email alert. Both are sent when the alert is triggered.
- **Schedule-dependent delivery**. You can also set different schedules for the different actions within the same alert definition. For example, you can schedule an email alert action to be sent during regular working hours and an SMS alert action for evening and night hours. Both are triggered by the same change in condition but are sent at different times, depending on when the alert is triggered.
- **Action dependencies**. You can also make one alert action dependent on another alert action. This enables you to instruct SiteScope to send one type of alert when the trigger condition is first met and send another type of alert only when the first type of alert has been sent a number of times.

You can copy an alert action into other monitors or groups for use by other alerts. To use alert actions for other alerts, you must copy the alert and paste it into another monitor or group. All the alert actions for the alert are copied into the new alert. You can then edit the alert to be triggered for the new target monitor or group.

For details on working with different alert types, see "Action Type Dialog Box" on page 1473.

Understanding When SiteScope Alerts Are Sent

SiteScope triggers the alert as soon as any monitor it is associated with matches the alert trigger condition. The trigger settings options in the Alert Action dialog box enable you to control when alerts are sent in relation to when a given condition is detected. For example, you can choose to have SiteScope send an alert only after an error condition persists for a specific interval corresponding to a given number of monitor runs. This is useful for monitors that run frequently that monitor dynamic, frequently changing environment parameters. In some cases, a single error condition may not warrant any intervention. For details about configuring trigger settings, see "Trigger Frequency Pane" on page 1492.

The following examples illustrate how different alert configurations send alerts after the error condition has persisted for more than one monitor run. It is important to note that the sample interval corresponds to how often the monitor is run. If a monitor runs every fifteen seconds and the alert is set to be sent after the third error reading, the alert is sent 30 seconds after the error was detected. If the monitor run interval is once every hour with the same alert setup, the alert is not sent until 2 hours later.

Example 1 - Always, after the condition has occurred at least N times:

Example 1a. An alert is sent for each time monitor is in error after condition persists for at least three monitor runs. Compare this with Example 1b below.

Alert setup	Always, after the condition has occurred at least 3 times								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=3 alert!	c=4 alert!	c=5 alert!	c=0	c=1	c=2

Example 1b. An alert is sent for each time monitor is in error after condition persists for at least three monitor runs. Shows how the count is reset when the monitor returns one non-error reading between consecutive error readings. Compare this with Example 1a above.

Alert setup	Always, after the condition has occurred at least 3 times								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=0	c=1	c=2	c=3 alert!	c=0	c=0

Example 2 - Once, after the condition has occurred exactly N times:

An alert is sent only once if monitor is in error for at least three monitor runs, regardless of how long the error is returned thereafter.

Alert setup	**Once, after the condition has occurred exactly 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 3 - Initially, after X times, and repeat every Y times:

Example 3a. An alert is sent on the fifth time monitor is in error and for every third consecutive error reading thereafter. Compare this with Example 3b below.

Alert setup	**Initially, after 5 times, and repeat every 3 times**								
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	**Initially, after 3 times, and repeat every 5 times**								
sample interval	0	1	2	3	4	5	6	7	8
status									
count	c=0	c=1	c=2	c=3 alert!	c=4	c=5	c=6	c=7	c=8 alert!

Example 4 - Configuring Multiple Alerts:

Because you can create multiple alerts and associate more than one alert to a monitor, you can tell SiteScope to take more than one action for a given situation. For example, you can create one alert that tells SiteScope to page you whenever any monitor returns an error status. You can then create another alert that tells SiteScope to run a script file to delete files in the /tmp directory on your server if your Disk Space Monitor returns an error. If your disk becomes too full, SiteScope would page you because of the first alert definition and would run the script to delete files in the /tmp directory because of the second alert definition.

SiteScope alerts are generated when there is a change in state for a monitor reading. Thus you can set an alert for OK or warning conditions as well as error conditions. One way to take advantage of this is to add two alerts, one alert on error, and one alert on OK. Set alerts to be sent after the condition is detected 3 time. For the OK alert, check the box marked **Only alert if monitor was previously in error at least 3 times**. This prevents unmatched OK alerts, such as when a monitor was disabled for any reason (manually, by schedule, or by **depends on**) and then starts up again. This can also be used so that an OK alert is only sent after a corresponding error alert was sent. With these two alerts, you get a page when a link or service goes down (monitor detects change from OK to error), and another when it comes back up (monitor detecting change from error to OK).

The following is an example of using two alerts with a monitor. An Alert on error sent once for error after condition persists for at least three monitor runs. Alert on OK sent once for good status after at least one error or warning interval.

Alert on Error Setup	**On** Error		**Once, after the condition has occurred exactly 3 times**						
Alert on OK Setup	**On OK**		**Once, after the condition has occurred 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!

After the monitor's status changes, the relevant status count is reset to zero.

Customizing Alert Templates

SiteScope uses templates when generating alert messages and reports. In most cases, you select the template you want to use in the Alert page when you create an alert. You can customize the existing templates or create your own by making a copy of an existing template. You customize the alert templates by adding or removing text, by adding property variables (as listed in the "SiteScope Alert Template and Event Properties Directory" on page 1451, or changing the order of text or property variables that are included in the template.

Tip: We recommend that you create custom alert templates using new file names. If you modify one of the default templates provided with SiteScope and save the changes to the same file, the changes that you make may be lost if you reinstall SiteScope or upgrade the SiteScope installation.

To make a custom alert template available to SiteScope, you must save any customized alert templates into the directory containing the templates for the applicable alert type. For the list of directory names containing SiteScope alert templates you can copy and customize, see "SiteScope Alert Templates Directory" on page 1450.

The templates in these groups are text files that include property variable markers. You use a text editor to create or modify these templates. The new templates saved into the directories shown become available to the applicable alert on the Alert page.

For details on customizing alert template settings, see "How to Customize an Alert's Message Content" on page 1446 and "How to Customize Alert Template Tag Styles" on page 1449.

Example - Typical Template Used for the Email Alert

The following is an example of the default template used for the Email Alert. The first section is the alert header. The first line in the alert header includes a link to the SiteScope installation which sent the problem. This provides you with a way to access the SiteScope installation reporting the problem.

Below the link is a block of text that further summarizes what caused the alert. This includes:

- The name of the monitor that triggered the alert.
- The group to which the monitor belongs.
- The alert status reported by the monitor.
- The sample ID number indicating how many times the monitor ran before the condition was reported.
- The time of day when the error occurred.

```
This alert is from SiteScope at <SiteScopeURL>
Monitor: <groupID>:<name>
Group: <group>
Status: <state>
Sample #: <sample>
Time: <time>
----------Detail ----------
<mainParameters>
<mainStateProperties>
```

The names that appear within <brackets> are property variable markers. When the alert is generated, SiteScope replaces these markers with the corresponding values of the variable for the monitor or monitor group that has triggered the alert.

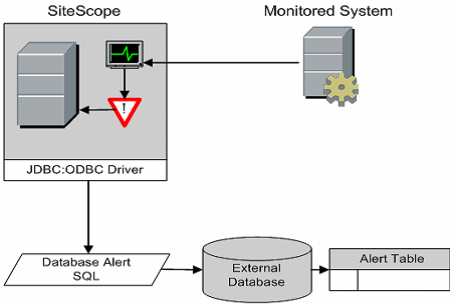
You add or edit the text portions of the template. For example, you could change the first line of the template above to read:

```
A Web monitoring alert was generated by the SiteScope installation found at
<SiteScopeURL>
```

Working with Database Alerts

Database alerts can forward system fault data and other status information to any SQL-compliant database.

The following diagram illustrates the Database alert.



You need the following to be able to use the Database alert type:

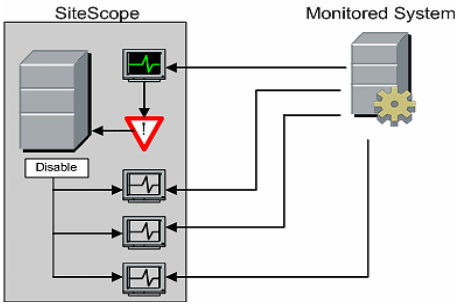
- Access to a SQL compliant database.
- The applicable database connection URL which the SiteScope server uses to connect to the database. For examples of common database connection URLs, see the "Setup Requirements and User Permissions" section for the relevant database monitor.
- Installation of the applicable database middleware driver that the SiteScope application uses to communicate with the database on the SiteScope server. For examples of common database driver strings, see the Setup Requirements and User Permissions section for the relevant database monitor.
- Database tables that have been created and structured to match the corresponding SQL statement that SiteScope uses to enter the alert into the database.

For details on how to configure an alert, see "How to Configure an Alert" on page 1443.

Working with Disable or Enable Monitor Alerts

Disable or Enable Monitor alerts can turn off and turn on the triggering of alerts for monitors. This is useful for times when server maintenance or other activities are being performed that would logically result in errors for some monitors and cause unnecessary alerts to be generated.

The following diagram illustrates an example of this alert type used to disable several monitors based on the condition reported to one monitor.

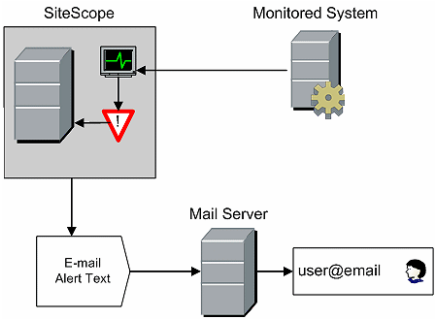


This alert type provides a functionality similar to the **Depends on** function for building group dependencies between monitors and monitor groups. One important difference is that monitors disabled by this type of alert are not automatically re-enabled when the status of the subject monitor or group changes back to the original state. You can create one alert with an **Alert Category** of **Error** that disables monitors. You can then create a second alert with an **Alert Category** of **Good** that enables the same monitors.

For details on how to configure an alert, see "How to Configure an Alert" on page 1443.

Working with Email Alerts

Email alerts send event notifications from SiteScope to a designated email address as seen in the following diagram.



You need the following to be able to use the Email alert type:

- Access to an active email server
- One or more email accounts that can receive the email alerts
- SiteScope Email Preferences set to work with the external email server

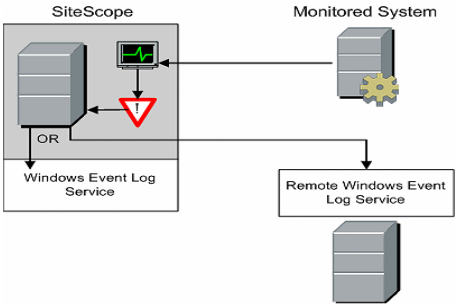
For more information on configuring SiteScope email recipients, see "Email Preferences" on page 791.

For details on how to configure an alert, see "How to Configure an Alert" on page 1443.

Working with Log Event Alerts

Log Event alerts can be used to extend the types of events that are logged to a Windows Application Event Log. This provides a way to forward event data to log query systems that may not normally be logged by the Windows operating system.

The following diagram illustrates the Log Event alert.



You need the following to be able to use the Log Event alert type:

- Access to the Windows Event Log service. By default, this is the Event Log on the machine where SiteScope is running. The alert definition can be configured to send log events to another server.
- SiteScope running on a Microsoft Windows platform.

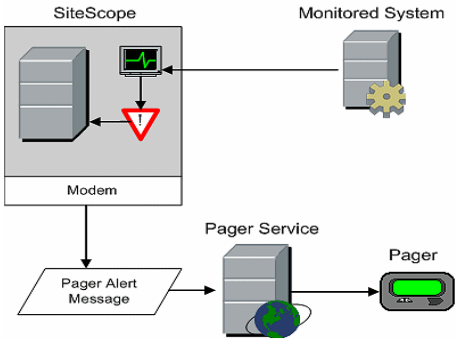
Caution: If you are using SiteScope's Microsoft Windows Event Log Monitor, you must use care when using the Log Event alert type because it is possible create an endless loop condition that can fill your Event log file. This can happen when a Microsoft Windows Event Log Monitor detects an event that triggers a Log Event alert, which in turn puts 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 Microsoft Windows Event Log Monitors.

For details on how to configure an alert, see "How to Configure an Alert" on page 1443.

Working with Pager Alerts

Pager alerts can be used to send event notification to electronic pagers. This is particularly useful when access to email may not be available. Depending on the type of pager you use and the capabilities of the pager service, you can configure the Pager Alert to send a pager message with an abbreviated description of the problem or detected condition.

The following diagram illustrates the Pager alert.



You need the following to be able to use the Pager alert type:

- Access to an active pager service
- A modem which the SiteScope server can use to connect to the pager service
- One or more pagers that can receive the pager alerts
- SiteScope Pager Preferences set to work with the modem and pager service

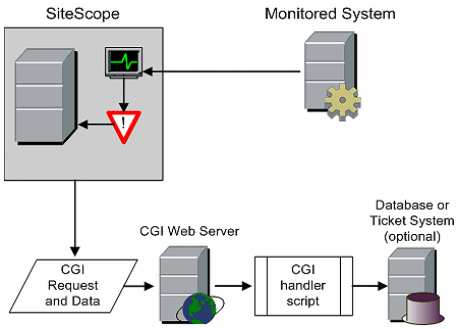
For more information on configuring SiteScope to use pager alerts, see "Pager Preferences" on page 801.

For details on how to configure an alert, see "How to Configure an Alert" on page 1443.

Working with Post Alerts

Post alert use the Common Gateway Interface protocol to forward POST data to a CGI enabled program. This can be used to forward event data to CGI script on another server that is a front-end for a trouble ticket system or reporting database. This alert type also provides a way of sending alert information through a firewall using HTTP or HTTPS without having to make other security changes.

The following diagram illustrates the Post alert.



You need the following to be able to use the Post alert type:

- HTTP access between the SiteScope server and the server running the CGI script or server.
- Format and syntax of the CGI POST request to the applicable CGI script or server.

For details on how to configure an alert, see "How to Configure an Alert" on page 1443.

Working with Script Alerts

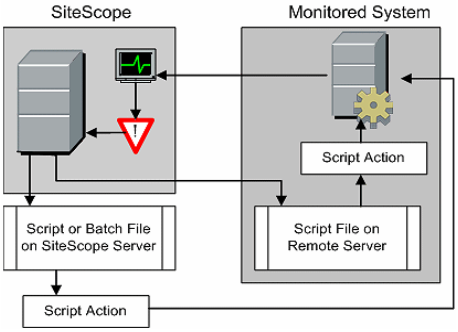
Script alerts can automatically initiate recovery scripts. You can configure a Script alert to run a command to restart a server or a service.

The most important components of Script Alerts are:

- The script definition itself.
- The monitor or monitors that are assigned to trigger the alert.
- The script to be run by the alert.

The alert message template and resulting alert message file may also need to be considered depending what the script needs to do. You can use a script template, together with the **Parameters** setting to pass data to your script.

The following diagram illustrates the general concept of the script alert for both a local script and a script on a remote host.



The script alert definition or instance and the monitor or monitors that trigger the alert are handled as with other alerts or monitors in SiteScope. For example, you may create a monitor to watch a Web server running on a remote UNIX server. You can create a Script Alert associated with that monitor that runs a script to kill and restart the Web server process if the monitor reports an error.

For details on how to configure an alert, see "How to Configure an Alert" on page 1443.

This section also includes:

Managing Script Files

Creating the script file to be called or run by the Script Alert definition is another key step in using this automation capability in SiteScope. The specific commands and actions taken by the script are up to you. The script file should be written as a plain text file compatible with the operating system where the script is to be run. This may be the same server where SiteScope is running or it may be on a remote machine to which SiteScope has access.

To run a script on the machine where SiteScope is running, the script file must be saved in the **<SiteScope root_directory>\scripts** directory on the SiteScope machine where the Script Alert is defined.

To run a script on a remote machine, you must save the script in a directory called **\scripts** in the home directory tree for the user account that SiteScope has execute permissions for on the remote machine.

The current execution directory when a script is run is **<SiteScope root directory>\classes** and not the **<SiteScope root directory>\scripts** directory. For commands run by the script itself, the relative execution directory is **<SiteScope root directory>\classes**. Use full paths for any other file system commands or programs called by your script so that you do not need to worry about the current directory. Also, the server system environment variables may not have been set up for the script execution. This is another reason to use full paths for executables called by the script. If a script works when you run it from the command line but not from SiteScope, then you must determine what the error is.

Passing Data to a Script

SiteScope passes a number of parameters to the script as command line arguments. You can use this option to pass data to a script that can be used to modify a script's action. This adds versatility to the Script Alert. By default, a SiteScope Script Alert passes seven command line arguments to a script. These are:

- The path of the scripts directory.
- The name of the monitor that caused the alert.
- The current status of the monitor.
- The path to the Alert Message File.
- The ID code of the monitor.
- The group the monitor is in.
- Any additional parameters specified on the **Parameters** text box in the alert form.

Two of these default arguments enable the script to access even more data. One is the Alert Message File and the other is the **Parameters** text box. The Alert Message File is a temporary text file created by SiteScope based on the alert template chosen for the Script Alert instance. Depending on the template you create or use, the Alert Message File may contain custom information as well as data specific to the monitor that triggered the alert. By passing the path to the Alert Message File to the script, you can have the script access this data.

You use the Parameters text box to specify individual monitor parameter data to be passed to the script. You can include multiple parameters by separating the parameters with spaces. This effectively enables you to increase the total number of parameters passed to the script.

The path of the scripts directory can be useful in setting a execution path to another program as well as setting a directory path for any output written by the script.

For more information and examples of passing parameters and data to scripts, see "Writing Scripts for Script Alerts" on page 1495.

Running Different Types of Scripts

You can run non-batch scripts, for example VBScript or Perl scripts, without wrapping them into a batch file (in versions of SiteScope earlier than 9.50, this was not possible).

- You can see scripts with any extensions by adding the _scriptMonitorExtensions property to the **master.config** file. For example, to see **.pl**, **.py**, or **.php** scripts, use the following format: _scriptMonitorExtensions=.pl;.py;.php
- You can run script interpreters with script extensions by adding the _scriptInterpreters property to the **master.config** file as follows: _scriptInterpreters=pl=c:/perl/perl.exe;py=c:/python/python.exe;php=c:/php/php.exe

Troubleshooting Scripts

This section describes troubleshooting and limitations when working with SiteScope scripts.

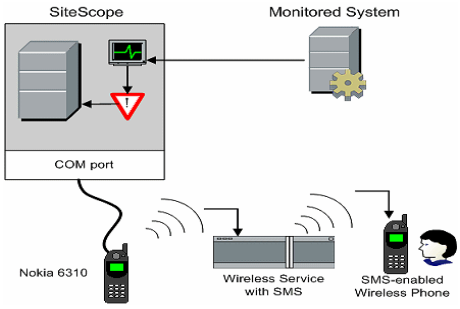
- The scripts are run with the permissions of the account used by the SiteScope service. Some scripts may need extra permissions and you must use the Services control panel to change the login account for SiteScope and then stop and start SiteScope. For example, scripts that restart services or reboot remote machines or scripts that copy protected files.
- Because the script is run by the SiteScope service, anything done as part of your login may not have occurred in the script. For example, you can not rely on mapped drives, environment variables, or other login script items. In addition, it cannot receive any interactive input from a keyboard or other input device. Any script action or command that requires a user confirmation or input would cause the script to hang. Do not include any interactive commands requiring a user action as part of the script. Also, opening a WIN32 application (for example, Notepad) also causes the script to hang because it is waiting for the user to exit or close the application before continuing with the script execution.
- If there are quotation marks in the Script Alerts status summary, SiteScope doubles the quotation marks in the Script Alert results. You should take this into account when defining a content match filter.

Working with SMS Alerts

SMS alerts are designed to transmit the name of the SiteScope monitor that has reported an event condition and the status of that monitor as the content of the message. It is an alternative to the Pager alert for communicating event notifications to mobile users without using email.

Note: At present, the SMS alert can only be sent from SiteScope by using the hardware specified in this section. For alternative ways of sending SMS messages using SiteScope, see the HP Software Self-solve knowledge base (http://h20230.www2.hp.com/selfsolve/documents). To enter the knowledge base, you must log on with your HP Passport ID.

The following diagram illustrates the SMS Alert.



You need the following to be able to use the SMS alert type:

- An available serial communications port on the SiteScope machine that is sending the SMS alerts.
- A serial-to-wireless device interface cable, RS-232 Adapter Cable Nokia DLR-3P to connect the wireless transmitting device to the machine where SiteScope is running.

- An SMS-enabled wireless device connected to the SiteScope machine that is sending the alerts (that is, the Nokia 6310 phone using the interface cable).
- The necessary software to enable the SMS Alert (normally included with SiteScope 7.6c1 and later).

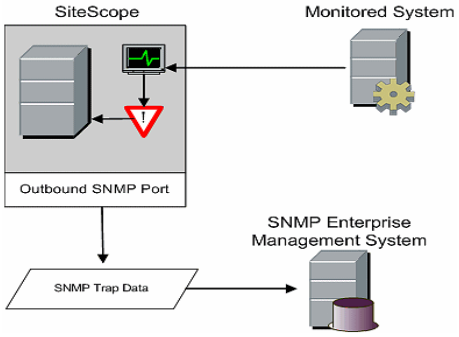
Note: Make sure that you do not have Nokia Data Suite, Palm Hot Sync, or any PDA software running on the server where SiteScope is running. These programs can bind the COM ports and prevent the dialer from working correctly.

For details on how to configure an alert, see "How to Configure an Alert" on page 1443.

Working with SNMP Trap Alerts

SNMP Trap alerts forward event data from any type of SiteScope monitor to an SNMP enabled host or management system. This means that SiteScope can be used to monitor and report events for applications and systems that do not have their own SNMP agent. For example, this can be used to send measurement data from a SiteScope Microsoft Windows Performance Counter based monitor type or a URL monitor in the form of an SNMP trap.

The following diagram illustrates the SNMP Trap Alert.



You need the following to be able to use the SNMP trap alert type:

- Access to the applicable SNMP network ports
- SiteScope SNMP Preferences set to work with the applicable SNMP management console

For more information on configuring SiteScope to use SNMP alerts, see "SNMP Preferences" on page 811.

For details on how to configure an alert, see "How to Configure an Alert" on page 1443.

Working with Sound Alerts

Sound alerts play a sound or audio file on the machine on which SiteScope is running when an alert is generated. The alert is effective only if the SiteScope server is in an area regularly occupied by support staff and the server is equipped with a sound card capable of processing the associated sound file.

Alternatively, SiteScope can be configured to embed an alert audio file into the Web pages served by SiteScope. This audio file is included with any SiteScope page that includes an error status for any monitor, such as the main pane or group detail pages. While this enables audio notification to all SiteScope clients through the user interface, it is not a true SiteScope alert and thus does not enable the same configuration options as the Sound Alert.

For details on how to configure SiteScope to play sounds through the browser, see the "Example - Configuring SiteScope to Play Sounds Through the Browser" on page 1448.

For other information on sound alerts, refer to the HP Software Self-solve knowledge base (h20230.www2.hp.com/selfsolve/documents). To enter the knowledge base, you must log on using your HP Passport ID.

For details on how to configure an alert, see "How to Configure an Alert" on page 1443.

Tasks

How to Configure an Alert

This task describes the steps involved in configuring an alert definition.

This task includes the following steps:

1 Create an alert

You can create a new alert or copy an existing alert into any group or monitor container in the SiteScope tree.

- **Create a new alert.** Right-click the container to which you want to associate the alert, and select **New > Alert**. Enter a name for the alert, select the targets to trigger the alert, and configure an alert action (in the **Alert Actions** pane, click **New Alert Action** to start the Alert Action wizard). For each alert scheme, you can create one or more alert actions. For user interface details, see "New/Edit Alert Dialog Box" on page 1463.
- **Copy an Alert Definition.** In the Alerts tab, select the alert you want to copy, and paste it into the desired group or monitor container. The alert target automatically changes to the group or monitor into which the alert is copied.

Caution: If you copy an alert definition from one group container to another, the **Alert targets** for the pasted alert are automatically reset to include all of the children of the container into which the alert is pasted. After pasting an alert, edit the alert definition properties to be sure that the assigned **Alert targets** are appropriate to the new alert context and your overall alerting plan.

---

2 Test the alert

Select the alert in the Alerts tab of the monitor tree and click **Test**. Select the monitor instance you want to test and click **OK**. A dialog box opens with information about the alert test.

Note: The monitor you select does not have to be reporting the same status category that is selected to trigger the alert to test the alert. For example, the monitor does not have to currently be reporting an error to test an alert that is triggered by error conditions.

---

3 Customize an alert's message content

Customize SiteScope alert templates to alter the content and format of alert messages.

For task details, see "How to Customize an Alert's Message Content" on page 1446.

4 Customize alert template tag styles

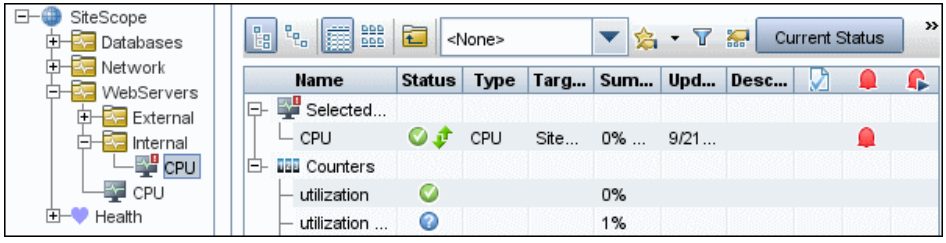
Customize SiteScope alert templates tag styles if you have a parser that needs a specific delimiter or to change the bracket delimiters used to identify variables.

For task details, see "How to Customize Alert Template Tag Styles" on page 1449.

5 Results

An alert is added to the specified container in the monitor tree (indicated by the icon). The alerts icon is also displayed in SiteScope Dashboard next to each group or monitor that has one or more configured alerts.

Example:



How to Customize an Alert's Message Content

This task describes how to customize SiteScope alert templates to alter the content and format of alert messages.

1 Open a text editor that has access to the alert template directories on the SiteScope machine.

For a list of the directory names containing SiteScope alert templates, see "SiteScope Alert Templates Directory" on page 1450.

2 Open an existing template file of the alert type you want to customize within a text editor.

3 Make changes to the template. Depending on the alert type, you can add or remove text, change the order of text or property variables, or add other property variables. To add specific properties, add the applicable property variable name between < > bracket pairs to the template.

For a list of specific property variables, see "SiteScope Alert Template and Event Properties Directory" on page 1451.

4 Save the changes to a unique filename within the directory for the applicable alert type. The new template is added to the Action Type Settings Template drop-down list.

Example - Shortening an Email Alert Message:

You can shorten the length of an email alert by removing properties that provide unneeded information. For example, if there is no added value in reporting the time of a specific alert, you can remove the <time> property from the template.

Tip: We recommend that you use the Typical template (the default setting) as a base for your customized template.

In the **<SiteScope root_directory>\templates.mail** directory, open the **Typical** template file. Remove the line Time: <time>. Save the changes to a new filename.

Example - Changing an SNMP Alert Message

You can change the SNMP Alert message from displaying the SNMP monitor's status to displaying a list of counters that are in Error state along with their values. This causes the message to only contain counters that breached the Error threshold and to omit all other counters.

In the <SiteScope root dir>\templates.SNMP directory, open the **Default** template file in a text editor. The file contains the line:
SiteScope\<group>\<name>\<sample>\<state>\

Replace the string <state> with the string <errorOnly>. The angle brackets (<,>) must remain around the text.

Note: If you want to display a list of counters that are in Warning state, replace the string <state> with the string <warningOnly>.

Edit <**SiteScope root dir**>**groups****master.config** file and add the line
_errorOnlyDelimiter=,

with other similar error definitions.

In this example, the delimiter is a comma (,), but you can also use a space (" ") or a tab (\t). The added line in **master.config** looks something like:

```
_errorSoundURL=
_errorOnlyDelimiter=,
_errorOnlyNewlineFormat=true
```

Note:

- If you used the string <**warningOnly**>, you must use the string _**warningOnlyDelimiter**=<**delimiter**> in **master.config**.
- If no _**errorOnlyDelimiter** is defined in **master.config**, the default delimiter is a space (" ").

Example - Configuring SiteScope to Play Sounds Through the Browser

You can configure SiteScope to play sounds in the browser to indicate a change in monitor status.

To enable playing sounds through the browser:

1. Open the <**SiteScope root directory**>**groups****master.config** file in a text editor.
2. Find the _errorSoundURL setting. (
3. Change the setting to:

   _errorSoundURL=http://<SiteScope host>:<SiteScope port>/SiteScope/templates.sound/alarm.au
4. Save the **master.config** file.
5. Stop and start SiteScope.
6. After this change, any time an error is triggered, SiteScope plays an alarm sound (in this case, **Alarm.au** from the <**SiteScope**>**templates.sound** directory). You can change the sound that is being played by modifying the source (src) in the tag above. If you want to add sound for warning or good status, then you can similarly change the _warningSoundURL= or _goodSoundURL= setting.

How to Customize Alert Template Tag Styles

This task describes how to change the delimiter between items in the list if, for example, you have a parser that processes alert messages and needs a specific delimiter. You can also change the bracket delimiters that are used to identify variables. This is useful if you want the message read by XML and a variable replaced by an XML string.

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}.

Reference

SiteScope Alert Templates Directory

The following is a list of the directory names containing SiteScope alert templates you can copy and customize.

Template Group	Description	Location
Event Log	Format and content of data written into event logs.	<SiteScope root directory>\templates.eventlog
History	Format and content of email messages that notify recipients that a report has been generated.	<SiteScope root directory>\templates.history
Email	Format and content of alert messages sent by email.	<SiteScope root directory>\templates.mail
Template	Group, Description, Location, Pager Format, and content of pager alerts.	<SiteScope root directory>\templates.page
Post	Format and content of messages submitted to a CGI script by a post alert.	<SiteScope root directory>\templates.post
Script	Format and content of messages sent to a script when a script alert is triggered.	<SiteScope root directory>\templates.script
SNMP	Format and content of messages sent by SNMP when a SNMP trap is triggered.	<SiteScope root directory>\templates.snmp

SiteScope Alert Template and Event Properties Directory

The following common properties can be found or used in SiteScope alert templates, common event mapping attributes, and in email reports.

This section includes:

Alert Template and Event Properties

The following is a list of the common properties found in SiteScope alert templates and common event mapping attributes.

Available Properties	Description / Example	Included in Templates
<_customPropertiesValues>		
<_eventCategory>		NTEventlog
<_httpPort>		NTEventlog
<_webserverAddress>		NTEventlog
<alert>		XMLMail
<alertHelpURL>	URL of the SiteScope help including the alert topic	NoDetails Traceroute WithDiagnostic
<alert::name>	The name of the alert	
<alert::id>	The alert ID	
<alert::description>	Text description for the alert definition	
<alert::disableDescription>	Description of the purpose of the disable operation	
<alert::actionID>	The ID for the alert action	
<alert::actionName>	The name of the alert action	

Available Properties	Description / Example	Included in Templates
<all>	All of the properties of the monitor	
<allThresholds>	Returns all the thresholds in the monitor in the email alert	
<automaticSeverityMapping>		
<bacMonitorID>	The monitor's BSM ID	
<bacSessionID>	The BSM profileID	
<category>	The monitor category	Typical
<_classifier>	Returns the first threshold in the monitor in the email alert	
<currentTime>	The time that the alert is run	
<diagnostic>		XMLMail
<diagnosticText>		Default User NoDetails WithDiagnostic
<diagnosticTraceRoute>		Traceroute WithDiagnostic
<errorCounterOnly>	List of the monitor counters in error status (returns counter name only)	
<errorOnly>	List of the monitor counters in error status (returns counter name and counter value)	Typical
<etiType>		
<etiValue>		
<eventID>		NTEventlog
<eventMachine>		NTEventlog

Available Properties	Description / Example	Included in Templates
<eventSource>		NTEventlog
<eventType>		NTEventlog
<firstgroupdescription>		
<fullMonitorName>		
<FullGroupId>	Full path from the SiteScope root directory to the group, exclude\SiteScope	
<goodCounterOnly>	List of the monitor counters in good status (returns counter name only)	Typical
<goodOnly>	List of the monitor counters in good status	Typical
<group>	Name of the group that the monitor is in	AllErrors Default Default User lr-Default_mail_ template NoDetails NTEventlogt PagerMail ShortMail Traceroute Typical WithDiagnostic XMLMail
<groupdescription>	Group description	

Available Properties	Description / Example	Included in Templates
<groupID>	ID of the group	Default Typical WithDiagnostic XMLMail
<id>		XMLMail
<mainParameters>	List of the main monitor properties that are set as parameter	Default Default User NTEventlog WithDiagnostic
<mainStateProperties>	List of main monitor properties that are set as state properties. These are the result statistics that are shown on the Reports.	Default Default User NTEventlog WithDiagnostic
<metric>		
<metricValue>		
<monitorDrilldownURL>	Creates a hyperlink in the event to the monitor URL.	
<monitor>		XMLMail
<monitorName>		
<monitorType>		

Available Properties	Description / Example	Included in Templates
<name>	Name of the monitor (same as _name)	Default Default User lr-Default_mail_template NoDetails NTEventlog PagerMail ShortestMail ShortMail ShortSubject Traceroute Typical WithDiagnostic XMLMail
<newSiteScopeURL>	URL of the SiteScope server	Default Typical
<newStatus>		
<oldStatus>		
<processtext>		
<remoteMachineName>	The name of the remote server machine	

Available Properties	Description / Example	Included in Templates
<sample>	Sample #	AllErrors Default Default User NoDetails NTEventlog PagerMail ShortMail Traceroute Typical Typical.mail WithDiagnostic XMLMail
<secondaryParameters>	Lists the main state properties and other internal properties	
<secondaryStateProperties>	Lists the main state properties and other internal properties	
<server>		XMLMail
<sitescope>		XMLMail
<sitescopeURL>	The URL to the main page of SiteScope for admin access	AllErrors Default User NoDetails Traceroute WithDiagnostic
<sitescopeuserurl>	The URL to the main page of SiteScope for user access	

Available Properties	Description / Example	Included in Templates
<state>	Status string reported by the monitor (same as stateString)	AllErrors Default Default User lr-Default_mail_ template NoDetails PagerMail ShortestMail ShortMail ShortSubject Traceroute Typical WithDiagnostic XMLMail
<tag>	Tags of the monitor (if exists)	Default Default User lr-Default_mail_ template NoDetails NTEventlog PagerMail ShortestMail ShortMail ShortSubject Traceroute Typical WithDiagnostic XMLMail

Available Properties	Description / Example	Included in Templates
<tag:[tagName]>	Displays the value or values of the Search/Filter tag with the [tagName] assigned to the monitor that triggered the alert. **Example:** You have a tag named AppServer with value Apache assigned to a monitor, and you include **<tag:AppServer>** in the alert template configured for that monitor. If an alert is triggered, the new property is replaced with Apache in the alert text.	
<targetHost>		
<thresholdCrossed>		
<time>	Time that the monitor completed the last run	AllErrors Default Default User lr-Default_mail_template NoDetails NTEventlog Traceroute Typical WithDiagnostic XMLMail
<time-date>	The date portion of the time that the monitor completed	
<time-time>	The time portion of the time that the monitor completed	

Available Properties	Description / Example	Included in Templates
<warningCounterOnly>	List of the monitor counters in warning status (returns counter name only)	
<warningOnly>	List of the monitor counters in warning status (returns counter name and counter value)	Typical

Email Report Properties

The following properties are applicable to the email templates stored in the **<SiteScope>\templates.history** directory:

Available Properties	Description
_httpPort	Port number used to access SiteScope
_webserverAddress	IP address for the SiteScope Server
basicAlertSummary	Basic information on what alerts have been triggered
detailAlert Summary	More detailed information on alerts
reportIndexURL	URL to the index page for the management report
reportPeriod	Time period for this report
reportURL	URL to the HTML version of the management report
summary	Summary and measurement information
textReportURL	URL to the comma-delimited file generated by SiteScope
userReportIndexURL	URL to the index page for a user-accessible report
userTextReportURL	URL to the comma-delimited file generated by a user-accessible report

Available Properties	Description
userXMLReportURL	URL to the XML file generated by a user-accessible report
xmlReportURL	URL to the XML file generated by the management report

SiteScope Alerts User Interface

This section includes:

SiteScope Alerts Page

This page displays information about the alerts associated with the selected monitor or group. Use this page to add, edit, or delete alert definitions.

To access	In the monitor or template tree, select a group or monitor that has the alert symbol displayed next to it. In the right pane, click the **Alerts** tab to display the alerts configured for the object.
Important information	➤ Alerts created for a specific monitor or group are displayed in the object's **Alerts on Monitor/Group** list. Targeted monitors or groups are displayed in the **Alerts Associated with Monitor/Group** list. ➤ 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. ➤ You can also use the SiteScope API when working with alerts. For details, see "Using the SiteScope Configuration API" on page 42.
Relevant tasks	"How to Configure an Alert" on page 1443
See also	"SiteScope Alerts Overview" on page 1417

User interface elements are described below:

UI Element	Description
	**Show Child Alerts.** Displays only those alerts that are direct children of the selected node.
	**Show All Descendent Alerts.** Displays all descendent alerts of the selected node.
	**New Alert.** Opens the New Alert dialog box enabling you to configure an alert, and add it to the selected SiteScope group or monitor. For user interface details, see "New/Edit Alert Dialog Box" on page 1463. **Note:** This button is available in the **Alerts on Monitor/Group** table only
	**Edit Alert.** Opens the Edit Alert dialog box enabling you to edit the properties of the selected alert. For user interface details, see "New/Edit Alert Dialog Box" on page 1463.
	**Copy.** Makes a copy of the alert. **Note:** This button is available in the **Alerts on Monitor/Group** table only.
	**Paste.** Pastes the alert to a selected location in the tree. **Note:** This button is available in the **Alerts on Monitor/Group** table only.
	**Delete Alert.** Deletes the alert from the tree.
	**Enable.** Enables the alert associated with the monitor/group.
	**Disable.** Disables the alert associated with the monitor/group.
	**Test.** Tests the alert definition on a selected server.
	**Select All.** Selects all listed alerts.

UI Element	Description
	**Clear Selection.** Clears the selection.
Name	The name by which the alert is known in SiteScope.
Status	The enabled/disabled status of the alert.
Description	A description of the alert.
Action Name	The name given to the alert action in the Action Type Dialog Box.

New/Edit Alert Dialog Box

This dialog box 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, and select **New** > **Alert**, or select an existing alert in the Alerts tab (monitor or template view) and click the **Edit Alert**  button.
Relevant tasks	"How to Configure an Alert" on page 1443
See also	➤ "SiteScope Alerts Overview" on page 1417 ➤ "Action Type Dialog Box" on page 1473 ➤ "Alert Action Dialog Box" on page 1476 ➤ "Common Event Mappings" on page 819

General Settings

User interface elements are described below:

UI Element	Description
Name	Name for this alert definition. This name is used to identify this alert definition in the product display.
Alert description	Description of the alert. This description does not appear in any other context. It appears only when editing the alert.

Alert Targets

User interface elements are described below:

UI Element	Description
Alert targets	Use the context menu tree to select the groups, monitors, or both, to trigger this alert. The context menu includes the currently selected object and all of the child objects. Check the box beside the current object to associate this alert with all objects within this object. Check one or more individual objects to associate this alert definition to the selected objects. 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. For details, see "Filter Settings" on page 1471.

Alert Actions

User interface elements are described below:

UI Element	Description
	**New Alert Action.** Opens the Action Type dialog box enabling you to define an action to be done when an alert is triggered. For user interface details, see "Action Type Dialog Box" on page 1473.
	**Edit Alert Action.** Opens the Action Type dialog box enabling you to edit the alert action. For user interface details, see "Action Type Dialog Box" on page 1473.
	**Delete Alert Action.** Deletes the alert action. It does not disable the associated monitors.
	**Duplicate.** Duplicates the alert action.
	**Select All.** Selects all listed alert actions.
	**Clear Selection.** Clears the selection.

UI Element	Description
 **<Alert Action Type icon>**	Indicates the type of action defined in the alert.
	 **Database.** Sends an alert message with a description of the problem as a record to a SQL database.
	 **Disable or Enable Monitors.** Manually controls the generation of alerts.
	 **Email.** Sends an email message to one or more email addresses with a description of the error or warning.
	 **Log Event.** Logs events to the Microsoft Windows Event Log.
	 **Pager.** Sends a message to a pager to signal that SiteScope has detected a particular condition.
	 **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 run scripts or batch files when the alert trigger condition is detected. The script or batch file that is called can run a system command or a program in any language that can be called from a command line entry.
	 **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.
Name	The name given to the action to be done when the alert is triggered. It is not the name of the alert.

UI Element	Description
Category	The category selected in the Status Trigger pane that triggers the alert action. For details on the Status Trigger user interface, see "Status Trigger Pane" on page 1491.
When	The schedule selected in the Trigger Frequency pane for when the alerts are sent. For details on the Trigger Frequency user interface, see "Trigger Frequency Pane" on page 1492.
Schedule	The daily or weekly schedule selected in the Action Type Settings pane. For details on the Action Type Settings user interface, see "Alert Action Dialog Box" on page 1476.
Target	Contains target data for the action type. Below you can see the content of the target column according to type: ➤ Email. Contains the email recipients selected in the **Send email to** section. ➤ Disable or Enable. Contains the targets selected in the **Targets** list. ➤ Database. Contains the URL entered in the **Database connection URL** box. ➤ Log Event. Contains the log event recipients selected in the **Send email to** section. ➤ Pager. Contains the pager recipients selected in the **Pager Alert Recipients** list. ➤ Post. Contains the URL entered in the **Post to url form** box. ➤ Script. Contains the script selected in the **Script** box. ➤ SMS. Contains the SMS number entered in the **SNMS number** box. ➤ SNMP Trap. Contains the SNMP traps selected in the **SNMP Trap** list. ➤ Sound. (The column is empty)

HP Operations Manager Integration Settings

Note: The HP Operations Manager Integration Settings pane is active only if the HP Operations agent is installed and connected to an HPOM/BSM server, and **Enable sending events** is selected in the HP Operations Manager Integration dialog box (**Preferences** > **Integration Preferences** > **HP Operations Manager Integration** > **HP Operations Manager Integration Main Settings**). For details, see "How to Enable SiteScope to Send Events to HPOM or BSM" on page 326.

User interface elements are described below:

UI Element	Description
Send events	Enables sending events to the HPOM/BSM server when an alert is triggered. **Default value:** Selected
Use monitor's event mapping	If selected, when an alert is triggered, SiteScope sends an event using the event mapping template associated with the monitor that triggered the alert. If cleared, SiteScope sends an event using the alert event attribute values. These values are filled according to the selected alert event mapping preference. The **Event mapping** setting below is available only when alert event mapping is used. **Default value:** Not selected

UI Element	Description
Event mapping	The event mapping template that is used for sending events for the monitor instance. The template contains mappings between SiteScope runtime data of the alert and the monitor that triggered the alert (metric level runtime data is not available) and the attribute values that are used for sending events. Select the desired event mapping template, or use the default mapping. Click **New** or **Edit** to open the Common Event Mappings dialog box and configure a new events preference or modify an existing one. For user interface details, see "New/Edit Event Mapping Dialog Box" on page 826. **Note:** This setting is active only when **Use monitor's event mapping** is cleared.
Event type indicator	You can enter an event type indicator for the alert that is sent with this event. This is the mapping between the measurement and its indicator. This is optional, and events without an indicator are still sent. Manually entering an indicator is useful since the CI type of a triggered alert is not always known when the alert is configured (for group alerts or alerts for monitors reporting CI type per metric). **Note:** The indicator cannot be resolved automatically, since the alert instance might be associated with more than one monitor or be triggered by more than one counter.
Event type indicator state	You can enter the event type indicator state that is sent with this event. This is the event severity level (Unknown, Normal, Warning, Minor, Major, Critical) that is mapped to the threshold that caused this status change. This field is optional, and events without an indicator state are still sent. **Note:** The indicator state cannot be resolved automatically, since the alert instance might be associated with more than one monitor or be triggered by more than one counter.

Enable/Disable Alerts

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.

User interface elements are described below:

UI Element	Description
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 alert for the next <time period>	Prevents the execution of the alert action for the time period you type, even if the alert condition is met. The alerts are disabled immediately and re-enabled when the time period expires.
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.
Disable description	(Optional) Description of the purpose of the disable operation.

Filter Settings

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 specific monitors within the selected list trigger the alert. This can simplify the creation of alert definitions and alert management. To disable alert filtering, clear the applicable fields and update the alert definition.

User interface elements are described below:

UI Element	Description
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 "Regular Expressions Overview" on page 236. ➤ 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.
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 type the text timeout, 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 "Regular Expressions Overview" on page 236. **Note:** The match is case sensitive.

UI Element	Description
Monitor type match	Limits the alert action to a monitor type from the set of monitors associated with this alert. Select the monitor types you want to include from the **Monitor Type List** and move them to the **Selected Monitor Type List** button.
Tags match	Limits the alert action to only those monitors associated with this alert that have the tag values selected. Select the tags you want to include.

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

Action Type Dialog Box

This dialog box enables you to select the action to be done when an alert is triggered.

To access	Right-click the SiteScope, group, or monitor for the alert, and select **New** > **Alert**, or select an existing alert in the Alerts tab (monitor or template view) and click the **Edit Alert** button. In the Alert Actions section of the New/Edit Alert dialog box, click the **New Alert Action** button.
Important information	➤ You can select only one type of alert at a time. ➤ If you are editing an alert, you cannot change the action type. For example, if an alert's action type was Email, you cannot change it to SMS.
Relevant tasks	"How to Configure an Alert" on page 1443
See also	➤ "SiteScope Alerts Overview" on page 1417 ➤ "New/Edit Alert Dialog Box" on page 1463 ➤ "Alert Action Dialog Box" on page 1476

User interface elements are described below:

UI Element	Description
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. For details on Database Alerts, see "Database Alert Properties" on page 1478.
Disable or Enable Monitors	Automatically enables or disables monitors or monitor groups based on a change of state in another monitor. **Note:** This action is not available when creating a template alert. For details on Disable/Enable Monitor Alerts, see "Disable or Enable Monitors Alert Properties" on page 1479.
Email	Sends an email message to one or more email addresses with a description of condition that triggered the alert. For details on Email Alerts, see "Email Alert Properties" on page 1481.
Log Event	Logs events to the Microsoft Windows Event Log. Entries in the event log can then be viewed with the Event Viewer and/or used by other software utilities that perform centralized alerting from the event log. For details on Log Event Alerts, see "Log Event Alert Properties" on page 1482.
Pager	Sends a message to a pager to signal that SiteScope has detected a particular condition. For details on Pager Alerts, see "Pager Alert Properties" on page 1484.
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. For details on Post Alerts, see "Post Alert Properties" on page 1485.

UI Element	Description
Script	SiteScope can run scripts or batch files when the alert condition is met. The script or batch file can run a system command or a program in any language that can be called from a command line entry. You can use this alert to run recovery scripts that automatically respond to critical conditions or failures (for example, to reboot a server or to copy files). For details on Script Alerts, see "Script Alert Properties" on page 1486.
SMS	Sends a short text message using the Short Message Service (SMS) to an SMS-enabled mobile phone or wireless device. For details on SMS Alerts, see "SMS Alert Properties" on page 1488.
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. For details on SNMP Trap Alerts, see "SNMP Trap Alert Properties" on page 1489.
Sound	Plays a sound or audio file on the machine on which SiteScope is running when an event has been detected. For details on Sound Alerts, see "Sound Alert Properties" on page 1490.

Alert Action Dialog Box

Use the Alert Action dialog box to define the settings that are specific to the alert type and to configure actions to be taken when an alert is triggered.

To access	Right-click the SiteScope, group, or monitor for the alert, and select **New** > **Alert**, or select an existing alert in the Alerts tab (monitor or template view) and click the **Edit Alert** button. In the Alert Actions section of the New/Edit Alert dialog box, click the **New Alert Action** button. In the Action Type dialog box, select an action type.
Important information	➤ The Action Alert dialog box consists of three panes: ➤ **Action Type Settings.** The Action Type settings vary according to the type of alert action you selected in the Action Type Dialog Box. For details of action types, see "Action Type Settings Pane" on page 1477. ➤ **Status Trigger.** For details, see "Status Trigger Pane" on page 1491. ➤ **Trigger Frequency.** For details, see "Trigger Frequency Pane" on page 1492.
Relevant tasks	"How to Configure an Alert" on page 1443
See also	➤ "SiteScope Alerts Overview" on page 1417 ➤ "New/Edit Alert Dialog Box" on page 1463

The following element is common to all action types:

UI Element	Description
New Variable	Click to define a new variable. For details, see "New Variable Dialog Box" on page 986. This button is available only from New/Edit Alert Dialog Box and New Action Dialog Box for template alerts.

Action Type Settings Pane

The contents of this pane depend on the action type you selected in the Action Type dialog box.

The following element is common to all action types in the Action Type Settings – the other elements are described in separate subsections:

UI 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. **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 General Settings to be Solaris_CPU and the action name to be send_sms.
New Variable	Click to define a new variable. For details, see "New Variable Dialog Box" on page 986.

Database Alert Properties

User interface elements are described below:

UI Element	Description
Database connection URL	Enter 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 type jdbc:odbc:test as the database connection URL. **Note for using Windows Authentication:** If you want to access the database using Windows authentication, type 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, because 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. 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>/java** directory. For more information about setting up database drivers for SiteScope, see "Database Query Monitor Overview" on page 114.
SQL statement	Enter 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>')
Database user name	Enter the user name to connect to the database if required.

UI Element	Description
Database password	Enter the password to connect to the database if required.
Backup database connection URL	If a backup database for SiteScope alert logging is required, enter the URL to the backup database connection to use if the main database connection fails. **Example**: If the ODBC connection for the backup database connection is called testdb2, the URL would be jdbc:odbc:testdb2.
Schedule	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. You can also use variables in this field. To do so, enter **%%** to display the list of available variables. **Default value:** every day, all day

Disable or Enable Monitors Alert Properties

User interface elements are described below:

UI Element	Description
Group/Monitors action	Select whether this alert action disables or enables a monitor when the alert is triggered. **Default value:** Disable

UI Element	Description
Targets	Select the groups and monitors that should be affected by the action of this alert. The **Targets** list includes all groups and monitors configured for the SiteScope. You can select any groups or monitors running in any group for this alert action and add them to the **Selected Targets** list. **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. **Default value:** None selected
Schedule	Select 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

Email Alert Properties

User interface elements are described below:

UI Element	Description
Send email to	Select email alert recipients using either of the following: ➤ **Recipients.** Select one or more Email recipients for the alert from the Email Alert Recipients list. The list displays the recipients that have been configured in Mail Preferences. For details, see "Email Preferences" on page 791. ➤ **Addresses.** Enter one or more email addresses separated by a comma (","). The addresses are checked for valid syntax according to the official standard RFC 2822, but not for other errors (for example, that the email user exists). **Note:** If the **Addresses** box contains data, selections from the Email Alert Recipients list are ignored. **Default value:** None selected
Subject	Select the subject field template for the email alert action message. The Typical template includes the following values: ➤ the subject of the message (SiteScope Alert) ➤ the category of the monitor alert (error, warning, ok, or no data) ➤ the name of the monitor or monitor title ➤ the status returned by the monitor ➤ the address, in parenthesis, of the SiteScope installation that sent the alert **Default value:** Typical **Example:** SiteScope Alert, error, URL: http://gate.company.com, unknown host name (gate.company.com)

UI Element	Description
Template	Select the template for the email alert action. In an Email alert action, select the **ShortMail** template for a shorter email message. Other options enable you to choose the level of detail to include in Email alerts. **Default value:** Typical. This template includes the following values: Monitor: <groupID>:<name>; Tags <tag>; Group: <group>; Status: <state>; Sample #: <sample>; Time: <time> **Note**: You can add additional templates into the **<SiteScope root directory>\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.
Schedule	Pre-defined schedules are displayed.
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:** Not selected

Log Event Alert Properties

User interface elements are described below:

UI Element	Description
Send to	Enter 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	Select the template for the log event type alert action. **Default value:** Typical **Note**: You can view the contents of the existing templates or add additional templates in **<SiteScope root directory>\templates.eventlog**.

UI Element	Description
Message	Enter the message prefix to be sent to the event log.
Event source	Enter the string used to set the <Source> field of the logged event. **Syntax:** must be text. **Default value:** SiteScope
Event ID	Enter the number used to set the <ID> field of the event that is logged. **Syntax:** must be numeric. **Default value:** 1000
Event type	Select the event type used for the event. **Default Value:** Use monitor status. This means that the Event Type is Error for an Error status, Warning for Warning, and Informational for monitors reporting a status of Good.
Event category ID	Enter a number to be used as the <category ID> for the event created by this alert. **Default value:** 0
Schedule	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. You can also use variables in this field. To do so, enter **%%** to display the list of available variables. **Default value:** every day, all day
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:** Not selected

Pager Alert Properties

User interface elements are described below:

UI Element	Description
Pager alert recipients	Select one or more pager recipients for the alert from the Pager Alert Recipients list. The list displays the recipients that have been configured in Pager Preferences. For details on this topic, see "Pager Preferences" on page 801. **Default value:** None selected
Template	Select the template for the pager alert action type. **Default value:** Typical **Note**: You can view the contents of the existing templates or add additional templates in the **<SiteScope root directory>\templates.page** directory.
Message	Enter the message text to be sent to the pager. **Note:** The maximum length is 32 characters.
Schedule	Pre-defined schedules are displayed.
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:** Not selected

Post Alert Properties

User interface elements are described below:

UI Element	Description
Post to URL form	Enter 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.
Template	Select the template for the post alert action type. **Default value:** Typical **Note**: You can view the contents of the existing templates or add additional templates in the **<SiteScope root directory>\templates.post** directory.
Authorization user name	Enter the user name to access the URL of the CGI script in a Post Alert. Not all CGI scripts require a user name. Alternatively, leave this entry blank and type the user name in the **Default authentication user name** section in the General Settings (**Preferences > General Preferences**). Use this method to define common authentication credentials for use with multiple monitors.
Authorization password	Enter the password for the Authorization user name in a Post Alert. Alternatively, leave this entry blank and type the password in the **Default authentication password** section in the **Preferences > General Preferences**. Use this method to define common authentication credentials for use with multiple monitors.
HTTP proxy	Enter the domain name and port of an HTTP Proxy Server used to access the URL of the CGI script.
Proxy server user name	Enter the user name to access the URL of the CGI script, if required by the proxy server. Your proxy server must support Proxy-Authenticate.

UI Element	Description
Proxy server password	Enter the password to access the URL of the CGI script, if required by the proxy server. Your proxy server must support Proxy-Authenticate.
Schedule	Select 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

Script Alert Properties

User interface elements are described below:

UI Element	Description
Server	Select the server on which the script should be run. The scripts directory must be in the directory tree of the remote login account that enables remote scripts to be run by SiteScope. **Default value:** SiteScope Server **Note when working in template mode:** The drop-down list is displayed as a text box to enable using a template variable in this field.
Script	Select the script to run in response to the selected condition. You can create as many custom scripts as you need. Place them in **<SiteScope root directory>\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. **Default value:** restartServer.bat

UI Element	Description
Parameters	Additional monitor parameters that you can pass to your script, such as: ➤ path of the scripts directory ➤ name of the monitor that caused the alert ➤ current status of the monitor ➤ path 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, type <_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 value:** No value. The Script Alert always passes the above parameters to a script as command line arguments. They do not need to be listed here.
Output encoding	Select the encoding of the script output. This enables SiteScope to match and display the encoded file content correctly. **Default value:** windows-1252
Template	Select the template for the script alert action type. **Default value:** Typical **Note**: You can view the contents of the existing templates or add additional templates in the <**SiteScope root directory**>**templates.script** directory.

UI Element	Description
Schedule	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. You can also use variables in this field. To do so, enter **%%** to display the list of available variables. **Default value:** every day, all day

SMS Alert Properties

User interface elements are described below:

UI Element	Description
SMS number	Enter the telephone number required by the SMS service that identifies the destination for the message. **Syntax:** Numeric only. Maximum of 16 digits.
Schedule	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. You can also use variables in this field. To do so, enter **%%** to display the list of available variables. **Default value:** every day, all day

SNMP Trap Alert Properties

User interface elements are described below:

UI Element	Description
SNMP Trap	Select one or more SNMP Traps to trigger an alert. **Default value:** None selected
Template	Select a template for the SNMP trap alert action type. Each line in the template is sent as a separate SNMP variable. The template file can also be modified using: ➤ [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 value:** Typical **Note:** You can view the contents of the existing templates or add additional templates in the <**SiteScope root directory**>**templates.snmp** directory.
Message	Enter an optional prefix to be added to the SNMP trap sent by this alert.

UI Element	Description
Schedule	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. You can also use variables in this field only for template alerts. To do so, enter **%%** to display the list of available variables. **Default value:** every day, all day
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.

Sound Alert Properties

User interface elements are described below:

UI Element	Description
Sound file	Select the sound to be played from **<SiteScope root directory>\templates.sound** directory. Additional sounds can be added to the directory in AU format (8 bit, &#micro;law, 8000 Hz, one-channel) with an .au suffix. **Default value:** Default
Schedule	Select the daily and weekly schedule to perform the alert action if the alert conditions are met and the alert is triggered. You can also use variables in this field. To do so, enter **%%** to display the list of available variables. **Default value:** every day, all day

Status Trigger Pane

Use the Status Trigger pane to select the status of the object type that triggers an alert action. Alerts are triggered when the status changes from one state to another. Select the category that triggers the alert action.

User interface elements are described below:

UI Element	Description
Unavailable	Alerts are triggered if the monitored machine was previously available and is currently no longer available.
Error	Alerts are triggered if the monitor was previously reporting a status of Good (default setting).
Warning	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.

Trigger Frequency Pane

Use the Trigger Frequency pane to select the trigger frequency.

Important information	➤ The available options vary according to what you chose in the Status Trigger Pane. ➤ For more detailed information on the options here, see "Understanding When SiteScope Alerts Are Sent" on page 1422.

User interface elements are described below:

UI 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 Email alert to be sent when the sound alert action has been triggered 3 times. Select the name of the sound alert action and 3. **Note**: This option is displayed 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. **Syntax:** numeric only **Range:** 1-99

UI Element	Description
Once, after the condition has occurred 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. **Default value:** Selected **Syntax:** numeric only **Range:** 1-99
Initially after <X> times, and repeat every <Y> times	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 Status Trigger pane. The alert is triggered only after any monitor in the group has reported the alert condition exactly N consecutive times. **Note:** This option is available only for SiteScope groups.

UI Element	Description
Once, after all monitors in this group are in error	This is displayed if you chose **Error** in the Status Trigger pane. The alert is triggered the first time all monitors in the group are in error. **Note:** This option is available only for SiteScope groups.
Only alert if monitor was previously in error/warning at least <N> times	This is displayed if you chose **Good** or **Warning** in the Status Trigger pane. 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

70

Writing Scripts for Script Alerts

This chapter includes:

Concepts

Concepts

Writing Scripts for Script Alerts Overview

SiteScope has the ability to run scripts or batch files when an error or warning status is detected. This is normally done by creating a Script Alert that acts as a trigger for the script. The script or batch file can run any system command or call other programs written in any language. You can use this to create recovery scripts to automatically respond to critical conditions or failures.

For a list of the common properties found in SiteScope alert templates, see "SiteScope Alert Template and Event Properties Directory" on page 1451.

Working with Scripts in SiteScope

The script file that a SiteScope Script alert is to run must be located in the **<SiteScope root directory>\scripts** folder or on a remote UNIX machine (for remote scripts). For example, if SiteScope is installed in the directory C:\SiteScope and your script is called actionTest.bat, SiteScope tries to run the following command line in response to Script Alerts you have created:

```
C:\SiteScope\scripts\actionTest.bat C:\SiteScope\scripts monitor_name
```

where C:SiteScope\scripts is the first command line parameter, monitor_name is the second command line parameter, and so forth.

Note: While the local script run by the Script Alert must reside in **<SiteScope root directory>\scripts**, the execution path is **<SiteScope root directory>\classes** directory. You should use full paths for any file system commands or programs called by the script to avoid problems with defining the current execution directory.

The action taken by a script is determined by the creator of the script. SiteScope passes several command line arguments to each script called by a Script Alert. You can use this to have program scripts take action based on information sent from SiteScope. By default, SiteScope passes the following parameters to each Script alert as command line arguments:

- The path of the scripts directory.
- The name of the monitor that caused the alert.
- The current status of the monitor.
- The path to the alert message file.
- The ID code of the monitor.
- The group in which the monitor is located.
- Any additional parameters specified in the **Parameters** box in the alert form.

These command line arguments can be accessed by the target script using the normal command line variable conventions. These conventions are %1, %2, %3 and so forth, for Windows NT systems, and $1, $2, $3 and so forth, for UNIX scripts (depending on the scripting shell or language used). The first six parameters (that is, %1 through %6) are passed by default to each script. To pass other parameters, the property variables or parameters must be added to the Script Alert Settings in the Parameters box to make them available to the script. The first variable or text entered in the Parameters box is then accessible as %7 by the script, the second parameter is accessed as %8, and so forth.

An example script written in Perl to access Script Alert parameters:

```
print "pathname to scripts directory: $ARGV[0]\n";
print "name of monitor causing alert: $ARGV[1]\n";
print "current status monitor: $ARGV[2]\n";
print "pathname to alert message file: $ARGV[3]\n";
print "id code of monitor: $ARGV[4]\n";
print "group for the monitor: $ARGV[5]\n";
```

The following is an example batch file for Microsoft Windows to echo the parameters passed to the script:

```
echo pathname to scripts directory: %1
echo name of monitor causing alert: %2
echo current status monitor: %3
echo pathname to alert message file: %4
echo id code of monitor: %5 echo group for the monitor: %6
```

Passing Data from SiteScope to a Script

In addition to the seven default parameters, there are two other mechanisms for passing parameters and data to scripts. One is to use the additional Parameters box in the Script Alert Settings. The other is to access the Alert Message file.

This section also includes:

- "Passing Data Using the Script Alert Settings" on page 1498
- "Passing Data Using the Alert Message File" on page 1500

Passing Data Using the Script Alert Settings

The simplest way to send additional custom parameters and data to script is to use the Alert Action dialog box. The seventh default parameter passed to the script, which is any additional parameters specified on the alert form, enables you to specify one or more custom parameters to be sent to the script. You specify these for a Script Alert in the **Parameters** box on the Action Types Settings pane of the Alert Action dialog box.

These parameters could be hard-coded values. You can include multiple parameters by separating the individual parameters by spaces. For example, assume you want to pass the four text strings shown below to a script. To do this you type them in the Parameters box as follows:

These would then become the seventh (7th) through tenth (10th) command line parameters sent to the script. The following Windows batch file script would print the default parameters as well as the additional example custom parameters entered in the Parameters box of the Action Types Settings Page:

```
echo pathname to scripts directory: %1
echo name of monitor causing alert: %2
echo current status monitor: %3
echo pathname to alert message file: %4
echo id code of monitor: %5
echo group for the monitor: %6
echo seventh parameter(customA): %7
echo eighth parameter(customB): %8
echo ninth parameter:(customC) %9
echo tenth parameter(customD): %10
```

Passing Data Using the Alert Message File

The other method for passing data and SiteScope monitor parameters to a script is to use the Alert Message file. This is a file that is created by SiteScope using the alert template specified in the Alert Action dialog box. You can create your own custom alert templates and pass custom text strings or any of the SiteScope parameters available. The following shows the default NTEventLog template included with SiteScope. The parameters marked with < > brackets are replaced with the applicable values to and written to the Alert Message file each time the applicable Script Alert is triggered. For a list of the common properties found in SiteScope alert templates, see "SiteScope Alert Template and Event Properties Directory" on page 1451.

```
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 1496). Then the script has to parse the content of the Alert Message file to extract the data you want to use in your script.

For more examples of how to write recovery scripts, look at the script files in the **<SiteScope root directory>\scripts** directory. You can use the **actionTest.bat** example template to create your own script. The **perlTest.pl** example shows how to call a Perl script. The **restartIIS.bat**, **restartService.bat**, and **restartServer.bat** scripts implement common recovery actions.

For the UNIX environment, the examples scripts are called action **Test.sh** and **perlTest.pl**.

71

SiteScope Reports

This chapter includes:

Concepts

Tasks

Reference

Concepts

SiteScope Reports Overview

SiteScope reports display information about how the servers and applications you are monitoring have performed over time. SiteScope reports are important tools in monitoring and troubleshooting operational performance and availability and reviewing the monitored environment.

You can create a report for a single monitor, several monitors, or even a number of monitor groups. Report definitions include report content options such as tables of specific monitor measurements, summaries of results, and graphs.

SiteScope reports can be valuable to many people in your organization, including management personnel in Sales, Marketing, Customer Support, and Operations. SiteScope User accounts can be created to enable these users restricted access to the SiteScope service to view reports. For more information, see "User Management Preferences Overview" on page 846.

Note:

- To view certain report elements on SiteScope for UNIX/Linux, it is necessary that an X Window system be running on the server where SiteScope is running.
- To be able to open reports generated in SiteScope version 9.0 and later after upgrading the SiteScope installation, you should create a manual backup of the reports folder **<SiteScope root directory>\htdocs**, and copy it to the new installation directory.
- Indicator values are not displayed in SiteScope reports.

SiteScope Monitor Data Log Files

SiteScope monitor data available for generating reports is limited to the amount of log data stored on the SiteScope server. By default, SiteScope retains monitor data log files for 40 days. The log files are rotated and files older than the log retention period are automatically deleted.

Note: Keeping monitor data logs for longer periods can cause a data storage problem for the SiteScope server depending on the total number of monitors configured and how often the monitors run per day. You should monitor the size of log files in the <**SiteScope root directory**>**logs** directory to estimate the data accumulation rate.

You can change the length of time that SiteScope retains monitor data using the log preferences. You can configure SiteScope to export monitor data to an external SQL-compliant database to maintain monitor data for longer periods or to make the data available to other reporting applications. For details, see "Log Preferences Overview" on page 784.

SiteScope Report Types

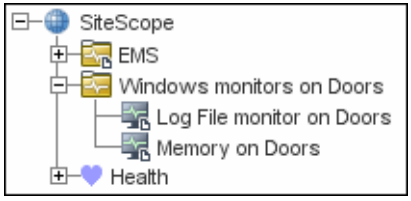
SiteScope includes four kinds of management reports. The following describes the report types and their usage.

Report Type	Description
Alert Reports	Alert reports provide information about SiteScope alerts generated during a specified period of time. You create an Alert report on an ad hoc basis. In addition, the settings for an Alert report are not saved to the SiteScope configuration data for later use. For details on configuring the Alert report, see "New SiteScope Alert Report Dialog Box" on page 1536.
Management Reports	Management reports provide a summary of infrastructure availability and performance data for a given period of time. Management reports are generated automatically based on their preset schedule from data collected by SiteScope monitors. According to the preset schedule, SiteScope reads the applicable log files and generates the report based on the monitor metrics for the time interval specified. You can save the report data in a file suitable for exporting to third-party applications. For details on configuring the Management report, see "New/Edit SiteScope Management Report Dialog Box" on page 1513.
Monitor Reports	Monitor reports enable you to review configuration properties and settings for existing monitors. You can export a monitor report in one of three text data formats. Unlike a Management report which is based on a schedule that you specify, you create a Monitor report on an ad hoc basis. In addition, the settings for a Monitor report are not saved to the SiteScope configuration data for later use. For details on configuring the Monitor report, see "New SiteScope Monitor Report Dialog Box" on page 1533.

Report Type	Description
Quick Reports	Quick reports enable you to view monitor data for specific monitors or groups of monitors during specific time periods. Unlike a Management report that is generated based on a schedule that you specify, you create a Quick report on an ad hoc basis. In addition, the settings for a Monitor Summary report are not saved to the SiteScope configuration data for later use. For details on configuring the Quick report, see "New SiteScope Quick Report Dialog Box" on page 1527.
BSM Configuration Changes Report	Displays statistics about the configuration reporting to BSM. It should be used for troubleshooting purposes only. The report is generated from BSM. If there are multiple SiteScopes reporting to BSM, the information displayed in this report includes information not only for the specific SiteScope selected. **Example**: The report logs exceptions, such as a failure to enter data into the profile database. **Note**: The report is available only when accessing SiteScope from SAM Admin and if the user has permission to view SiteScope logs.

Working with SiteScope Management Reports

Reports are added as elements to the Reports tab in the monitor view. They can be added as a child to the SiteScope node, to a group, or to an individual monitor. Reports are displayed in the left menu tree by a icon next to the group or monitor for which it was created, as shown in the example below.



Reports have a scope based on the container to which they are added. You add a report to the container or element that contains all of the monitors whose data you want to include in the report. You then use the **Report Targets** pane to narrow the selection of monitors to be included in the report.

When you select a node with a report icon, the Report tab displays two tables. The **Reports on** table displays the reports created on this node. The **Reports Associated with** table displays the reports created on an ancestor node and applied to this node using the target selection.

You can create as many SiteScope report definitions as you want. However, you should plan and consolidate reports to keep the number of report definitions to a minimum. This can facilitate report administration and help reduce redundant report messages or actions. When creating a report for a large number of monitors, you should consider making separate reports based on the type of monitor or measurement. For example, when reporting on system resources for 20 different remote servers, consider making one report with monitors that measure numeric values such as CPU or disk space and another report for monitors that report basic availability such as services or processes.

By default, SiteScope keeps the 10 most recently generated reports. This means that hourly reports are available for the last 10 hours, daily reports are available for 10 days, weekly reports are available for 10 weeks, and so forth. You can change this report storage period by changing the value of the _maximumReports setting in the SiteScope **master.config** file.

Deleting a Management report definition discontinues the generation of applicable report. Previously generated reports continue to be available until the underlying data is removed.

You can copy and paste a report definition. The report definition settings are pasted to the new location with the exception of the **Report targets** setting, which are automatically reset to include all of the children of the container into which the report is pasted. After pasting a report, you should edit the report definition properties to be sure that the assigned **Report targets** are appropriate to the new report context and your overall reporting plan.

Tasks

How to Create a Report

This task describes the steps involved in creating a SiteScope report.

This task includes the following steps:

- "Select a report type" on page 1508
- "Configure the report settings" on page 1508
- "Results" on page 1509

1 Select a report type

Right-click the group or monitor container in which you want to create a report, and click **Reports**, or create a new report from the Reports tab. Select the report type you want to add or generate (only the Management report is added; all other reports are ad hoc and are not saved in SiteScope).

For details of report types, see "SiteScope Report Types" on page 1504.

2 Configure the report settings

Select the monitors to include in the report and configure the report settings.

For user interface details, see "SiteScope Reports User Interface" on page 1510.

Note: By default, a report includes data from all monitors within the selected container. For Alert Reports, you cannot remove any of the monitors in the selected container from the report.

---

3 Results

Management reports are added to the selected container in the monitor tree (indicated by a report symbol). For details on viewing the Management report, see "Management Report" on page 1538.

All other reports are generated and displayed in your Web browser.

- For details on viewing the Alert report, see "Alert Report" on page 1548.
- For details on viewing the Monitor report, see "Monitor Summary Report" on page 1546.
- For details on viewing the Quick report, see "Quick Report" on page 1542.

Reference

SiteScope Reports User Interface

This section includes:

Reports Page

This page displays information about the reports defined in SiteScope. Use this page to add, edit, or delete report definitions. If a report has been set up for a SiteScope object (group or monitor), the report symbol is displayed next to the object icon in the monitor tree.

To access	Select the **Monitors** context. In the monitor tree, click the **Reports** tab. Select the SiteScope object to display report properties for the specific object.
Important information	Reports created for a specific monitor or group are displayed in the object's **Reports on Monitor/Group** list. Targeted monitors or groups are displayed in the **Reports Associated with Monitor/Group** list.

Relevant tasks	"How to Create a Report" on page 1508
See also	"Working with SiteScope Management Reports" on page 1506

User interface elements are described below:

UI Element	Description
	**Show Child Reports.** Displays only those reports that are direct children of the selected node.
	**Show All Descendent Reports.** Displays all descendent reports of the selected node.
	**New Report.** Enables you to select the type of report you want to configure. Only Management reports are added to the Reports tab (all other report types are created on an ad hoc basis, and are not saved in SiteScope). For details on the New SiteScope Management Report user interface, For user interface details, see "New/Edit SiteScope Management Report Dialog Box" on page 1513. **Note:** This button is available in the **Reports on Monitor/Group** table only.
	**Edit Report.** Enables you to edit the properties of the selected Management report. For details on the Edit Management Report user interface, see "New/Edit SiteScope Management Report Dialog Box" on page 1513.
	**Copy Report.** Makes a copy of the selected report. **Note:** This button is available in the **Reports on Monitor/Group** table only.
	**Paste Report.** Pastes the report to the selected location in the tree. **Note:** This button is available in the **Reports on Monitor/Group** table only.
	**Delete Report.** Deletes the selected Management report from the Reports tab.

UI Element	Description
	**Generate Report.** Generates a Management report for a selected monitor or group. For user interface details, see "Management Report" on page 1538.
	**Select All.** Selects all listed reports.
	**Clear Selection.** Clears the selection.
Type	Indicates the report type.
Title	The name by which the report is known in SiteScope.
Description	A description of the report.
Enabled	Indicates whether the generation of this report is enabled.
Path	Displays a link to the ancestor node that is targeting this object. **Note:** This column is available in the **Reports associated with** table only.

New/Edit SiteScope Management Report Dialog Box

This dialog box enables you to create a report that provides a summary of system availability data for a given time period.

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor, and select **Reports** > **Management**.
Important information	HTML code entered in report text boxes is checked for validity and security, and corrective action is taken to fix the code (for example, code is truncated if it spans more than one line). If malicious HTML code or JavaScript is detected, the entire field is rejected. The following is prohibited HTML content: ➤ Tags: **script**, **object**, **param**, **frame**, **iframe**. ➤ Any tag that contains an attribute starting with **on** is declined. For example, onhover. ➤ Any attribute with **javascript** as its value.
Relevant tasks	"How to Create a Report" on page 1508
See also	➤ "SiteScope Reports Overview" on page 1502 ➤ "Reports Page" on page 1510 ➤ "Management Report" on page 1538

General Settings

User interface elements are described below:

UI Element	Description
Report title	Enter a title for this Management Report. This name is used to identify this Management Report definition in the product display.
Description	(Optional) Use this text box to describe other information about this report definition. For example, include information about the purpose, target, setup date, or audience for this report.

Report Targets

User interface elements are described below:

UI Element	Description
Report targets	Select the groups, monitors, or both, to be included in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers. **Default value:** The current container and all child elements are selected.

Display Settings

User interface elements are described below:

UI Element	Description
Thresholds	
All thresholds	Creates a table of monitor error, warning, and good threshold settings for all of the monitors included in the report. If selected, this table is displayed as the first report section. **Default value:** Not selected
Error thresholds	Creates a table of individual error readings recorded by the monitors during the report period. **Default value:** Selected
Warning thresholds	Creates a table of individual warning readings recorded by the monitors during the report period. **Default value:** Selected
Good thresholds	Creates a table of individual good readings recorded by the monitors during the report period. **Default value:** Selected

UI Element	Description
Uptime and Readings	
Uptime Summary and Measurement Summary tables	Creates two report tables: **Uptime Summary** and **Measurement Summary**. For details of the data included in these tables, see "Report Content - Management Report Page" on page 1540. **Default value:** Selected
Uptime: Include warnings	Includes any monitor readings that are reported as warnings in the overall Uptime calculation. **Default value:** Not selected
Uptime: Ignore warnings	Suppresses 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 %. **Default value:** Not selected
Uptime: Ignore errors	Suppresses 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 %. **Default value:** Not selected
General	
Measurements graph	For graph reports, use the drop-down list to choose a graphical measurement to be included in the report. For details of the options, see "Graph Measurement Options" on page 1525.

UI Element	Description
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. **Default value:** Selected
Alerts table	Select an option to include a table of alerts sent for the monitors in the report. The options for the alerts table level are: ➤ **No alerts table.** No table of alerts is included in the report (default) ➤ **Basic alerts table.** Displays the time and summary information for each alert sent. ➤ **Show detailed alerts table for all alerts.** Displays detailed alert information for each alert in the report. ➤ **Show detailed alerts table for failed alerts.** Displays the time and summary information for each alert, and a full diagnostics breakdown for each failed alert.
Detailed monitor information	Displays all of the information gathered for each monitor on the report. Otherwise, only the primary data is displayed for each monitor. **Default value:** Not selected **Example:** If this box is checked on a URL Sequence Monitor, the timing information for each step in the sequence is displayed in the report.
Time in error	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. **Default value:** Not selected

Filter and Scheduling Settings

User interface elements are described below:

UI Element	Description
Monitor filter	Select a subset of those monitors to be shown in the report —those that have had the specified status sometime during the report's time frame. You can select only monitors in error or warning, monitors in error, monitors in warning, monitors that were OK, or all monitors. **Default value:** Show all monitors **Example:** Choosing **Show only monitors in error** displays report data only if that monitor had spent time in error sometime during the time interval of the report.
Schedule filter	Select a schedule filter option for showing only a subset of the data in the report—those monitors that have samples during the time period of the schedule. **Default value:** The report shows data for the full period of the report (every day, all day). **Example:** Choosing weekdays, 09:00-18:00 displays report data for the selected monitors with samples from the 9am to 6pm time period, Monday through Friday. Only this data is used for all the calculations.

UI Element	Description
Time period for report	Select the time period for which you want to view monitoring data. You can choose to report on data for a set number of hours, for the last day, the last several days, the past week, past month, or month-to-date for the current calendar month. 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. **Default value:** Last day
End of report period	Choose an end time for the report by selecting a time from the drop-down list. For example, you may want to have your reports run from midnight to midnight. **Default value:** At time report is run (SiteScope generates reports starting at the indicated time and ending at the time the report was generated)

Report Format

User interface elements are described below:

UI Element	Description
File format	This option enables some customization of the report appearance. The options are: ➤ **Color background** (default) ➤ **Color background, no table borders** ➤ **White background**

Report Distribution

User interface elements are described below:

UI Element	Description
HTML format	Select if you want the reports sent in HTML format. Use this option to include the SiteScope report graphics. If you do not select this option only a text summary of the report is sent. **Default value:** Not selected
Send report to email address	To have the report forwarded by email when it is generated, enter the email addresses to which this report should be sent each time its generated. To send the reports to multiple email addresses, separate the email addresses with commas.
Format template	Select a template for SiteScope to use to create the email message. You can choose from the following templates or make a copy of one of these and customize it to meet your own needs. ➤ **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** - Choose this option to send a history report. This is the default option. ➤ **HistoryMailAlertDetail** - Choose this option to have all alerts included in the report that is sent by email. ➤ **HistoryMailNoLinks** - Choose this option to send the report without any links in it.

UI Element	Description
Comma-delimited file	Select 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 root directory>\htdocs** directory. To find the exact location of the saved file on your machine, click the **View Report** tab for the report, and move the pointer over the **text** link for the report in the **Information For** column. The full path to the file is listed in the status bar of your Web browser. To open the saved file on your machine, click the **text** link to go to the Report page. If you enter an email address in the **Email** text box, SiteScope sends a copy of the comma-delimited file to that address. **Default value:** Not selected **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 email	If you enter an email address in the text box, SiteScope sends a copy of the file to that address.

UI Element	Description
XML file	Select this box to save a generated management report to an XML text file. SiteScope automatically saves these files in the <**SiteScope root directory**>**htdocs** directory. To find the exact location of the saved file on your machine, click the **View Report** tab for the report, and move the pointer over the **xml** link for the report in the **Information For** column. The full path to the file is listed in the status bar of your Web browser. To open the saved file on your machine, click the **xml** link to go to the Report page. If you enter an email address in the **Email** text box, SiteScope sends a copy of the comma-delimited file to that address. **Default value:** Not selected **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 email	If you enter an email address in the text box, SiteScope sends a copy of the XML file to that address.

Calculation Method

User interface elements are described below:

UI Element	Description
Time between samples	Use this time scale option to choose the time interval between monitor readings. You can choose intervals that range from once every minute to once a day, or you can use the automatic scaling. When automatic scaling is used, SiteScope determines how many readings were taken over the chosen time period for the given monitors and then selects an appropriate interval for the management report. **Default value:** Automatic time scale
Maximum graph value	Select a vertical scale option to choose the maximum value displayed on a graph. Choosing a specific scale value makes it easier to compare graphs from different monitors and times. **Default value:** Automatic vertical scale

Management Settings

User interface elements are described below:

UI Element	Description
Disable report	Select to temporarily disable the generation of this report. To enable the report again, clear the box. **Default value:** Not selected
Generate report at (HH:MM)	The time that you want SiteScope to create this management report. The report contains information for the last day, week, or month, ending at the time the report is run. For example, if a daily report is generated at 18:00 (6:00 p.m.), it contains data generated between 18:00 the previous day and 18:00 of the current day. The default value is 00:00 which represents midnight. **Default value:** 04:00 **Tip:** Try to schedule reports to be generated during off-peak hours relative to overall monitoring tasks and load, since report generation may temporarily affect overall SiteScope performance and responsiveness(depending on the number of monitors and time period of the report). If you are generating many reports each day, you should consider staggering the **Generate report at** value for different reports

Search/Filter Tags

User interface elements are described below:

UI Element	Description
<Tag name and values>	Keyword tags are used to search and filter SiteScope objects (groups, monitors, remote servers, templates, and preference profiles). If no tags have been created for the SiteScope, this section appears but is empty. If tags have been created, they are listed here and you can select them as required. For concept details, see "Working with Search/Filter Tags" on page 118.
Add Tag	Opens the New Tag dialog box, enabling you to add new keyword tags. For user interface details, see "New/Edit Tag Dialog Box" on page 129.

Note: A bar graph is generated using standard HTML, so it can be printed from all browser types. Line graphs are generated using a java applet and may not print directly from all browsers.

Graph Measurement Options

This table includes a description of the graph measurement options that can be included in the report:

Graph	Description
None - no graph	No graphs are included in 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 generated depends on whether the monitor records multiple measurements per monitor run (for example, the Microsoft Windows Resources or UNIX Resources monitor types) and whether the measurement types are compatibility with one another. Separate graphs are generated if the measurement types are not compatible.

Graph	Description
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.

Note: A bar graph is generated using standard HTML, so it can be printed from all browser types. Line graphs are generated using a java applet and may not print directly from all browsers.

New SiteScope Quick Report Dialog Box

This dialog box enables you to create a one-time SiteScope management report for any monitor or group of monitors over a given time period.

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor, and select **Reports** > **Quick**. Configure the report properties, and click **Generate Report**. Alternatively, you can create a report using preconfigured settings by selecting a monitor and clicking the **Quick Report** button in the SiteScope Dashboard.
Important information	➤ 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, edit the **Report period** setting. ➤ When working in BSM, Quick Report definitions in SAM Admin are stored only with the BSM context. Quick Report definitions are not stored in, and do not persist on the SiteScope server.
Relevant tasks	"How to Create a Report" on page 1508
See also	➤ "SiteScope Reports Overview" on page 1502 ➤ "Quick Report" on page 1542

Report Targets

User interface elements are described below:

UI Element	Description
Report targets	Select the groups, monitors, or both, to be included in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers. **Default value:** The current container and all child elements are selected.

Display Settings

User interface elements are described below:

UI Element	Description
Thresholds	
All thresholds	Creates a table of monitor error, warning, and good threshold settings for all of the monitors included in the report. If selected, this table is displayed as the first report section. **Default value:** Not selected
Error thresholds	Creates a table of individual error readings recorded by the monitors during the report period. **Default value:** Selected
Warning thresholds	Creates a table of individual warning readings recorded by the monitors during the report period. **Default value:** Selected
Good thresholds	Creates a table of individual good readings recorded by the monitors during the report period. **Default value:** Selected
Uptime and Readings	
Uptime Summary and Measurement Summary tables	Creates two report tables: **Uptime Summary** and **Measurement Summary**. For details of the data included in these tables, see "Report Content" on page 1543. **Default value:** Selected
Uptime: Include warnings	Includes any monitor readings that are reported as warnings in the overall Uptime calculation. **Default value:** Not selected

UI Element	Description
Uptime: Ignore warning	Suppresses monitor readings reported as warnings from the overall Uptime and Readings Summary section. **Default value:** Not selected **Note:** This option only suppresses the display of the Warning % column in the table; it does not change the calculation of the Uptime %.
Uptime: Ignore errors	Suppresses monitor readings reported as errors from the overall Uptime and Readings Summary section. **Default value:** Not selected **Note:** This option only suppresses the display of the Error % column in the table; it does not change the calculation of the Uptime %.
General Settings	
Measurements graph	For graph reports, use the drop-down list to choose a graphical measurement to be included in the report. For details of the options, see "Graph Measurement Options" on page 1525. **Default value:** Bar Graph - one graph per measurement
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. **Default value:** Selected

UI Element	Description
Alerts table	Select an option to include a table of alerts sent for the monitors in the report. The options for the alerts table level are: ➤ **No alerts table.** No table of alerts is included in the report (default). ➤ **Basic alerts table.** Displays the time and summary information for each alert sent. ➤ **Show detailed alerts table for all alerts.** Displays detailed alert information for each alert in the report. ➤ **Show detailed alerts table for failed alerts.** Displays the time and summary information for each alert, and a full diagnostics breakdown for each failed alert.
Detailed monitor information	Displays all of the information gathered for each monitor on the report. Otherwise, only the primary data is displayed for each monitor. **Example:** If this box is checked on a URL Sequence Monitor, the timing information for each step in the sequence is displayed in the report. **Default value:** Not selected
Time in error	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. **Default value:** Not selected

Filter and Scheduling Settings

User interface elements are described below:

UI Element	Description
Monitor filter	Select a subset of those monitors to be shown in the report —those that have had the specified status sometime during the report's time frame. You can select only monitors in Error or Warning, monitors in Error, monitors in Warning, monitors that were OK, or all monitors. **Default value:** Show all monitors **Example:** Choosing **Show only monitors in error** displays report data only if that monitor had spent time in error sometime during the time interval of the report.
Schedule filter	Select a schedule filter option for showing only a subset of the data in the report—those monitors that have samples during the time period of the schedule. **Default value:** The report shows data for the full period of the report (every day, all day). **Example:** Choosing **weekdays, 09:00-18:00** displays report data for the selected monitors with samples from the 9am to 6pm time period, Monday through Friday. Only this data is used for all the calculations.
Report period	Specify the time period for which you want to view monitoring data. Enter the time from which you want the report coverage to start in the **From** boxes and the time to which you want to cover in the **To** boxes. **Default value:** The time period is from one hour before the time that the Quick Report is generated until the current time. You can set the default time period for including monitoring data in the Quick report by configuring the **Default time length for report (hours)** setting in **Preferences** > **Infrastructure Preferences** > **Report Settings**. **Note:** Times should be entered in 24-hour format.

Report Format

User interface elements are described below:

UI Element	Description
Report in	Select the format to be used in displaying the report: HTML format, Text format or XML format. **Default value:** HTML format
File format	This option enables some customization of the report appearance. The options are: ➤ **Color background** (default) ➤ **Color background, no table borders** ➤ **White background**

Report Distribution

User interface elements are described below:

UI Element	Description
Send report to email address	To have the report forwarded by email when it is generated, enter the email addresses to which this report should be sent each time its generated. To send the reports to multiple email addresses, separate the email addresses with commas.

Calculation Method

User interface elements are described below:

UI Element	Description
Time between samples	Use this time scale option to choose the time interval between monitor readings. You can choose intervals that range from once every minute to once a day, or you can use the automatic scaling. When automatic scaling is used, SiteScope determines how many readings were taken over the chosen time period for the given monitors and then selects an appropriate interval for the management report. **Default value:** Automatic time scale
Maximum graph value	Select a vertical scale option to choose the maximum value displayed on a graph. Choosing a specific scale value makes it easier to compare graphs from different monitors and times. **Default value:** Automatic vertical scale

New SiteScope Monitor Report Dialog Box

This dialog box enables you to create a report that provides detailed information about the monitors defined in one or more monitor groups.

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor, and select **Reports** > **Monitor**.
Relevant tasks	"How to Create a Report" on page 1508
See also	➤ "SiteScope Reports Overview" on page 1502 ➤ "Monitor Summary Report" on page 1546

Report Targets

User interface elements are described below:

UI Element	Description
Report targets	Select the groups, monitors, or both, to be included in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers. **Default value:** The current container and all child elements are selected.

Display Settings

User interface elements are described below:

UI Element	Description
Display columns	Select the monitor information to display in the report columns. Data is shown in the report for the selected parameters only if the particular option has been selected, such as Disabled and Frequency, or if a value has been supplied, such as Monitor Description. If the option or value has not been defined in the particular monitor setup, the column is blank for that parameter for that monitor. **Note:** Hold down the SHIFT key to select a set of adjacent groups. Use CTRL-click to select non-adjacent items.
Show parameters	Select if you want the report to contain the parameters defined for each monitor. This option includes a list of the active options defined for each selected monitor in a single table cell rather than individual columns as with the option above. **Default value:** Selected

UI Element	Description
Sort by	Select the monitor parameter to use as a sort key for the report. **Default value:** Monitor Type
Sort order	Select the order to use for sorting the report. For example, to sort the report alphabetically by monitor type, select Monitor Type, and select Ascending sort order. **Default value:** Ascending

Export Settings

User interface elements are described below:

UI Element	Description
Export to file	Select this box to have SiteScope export the Monitor Summary report data to a text file. **Default value:** Not selected
File name	When the **Export to file** option is enabled, SiteScope writes the data to the file name specified here using the selected text format. The file is written into the **<SiteScope root directory>\htdocs** directory. **Default value:** monSummary
File format	Select the format for the exported file. The options are comma-delimited text, tab delimited text, or HTML. **Default value:** comma-delimited (csv)

New SiteScope Alert Report Dialog Box

This dialog box enables you to create a report used to display SiteScope alerts sent over a given time period.

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor, and select **Reports** > **Alert**.
Relevant tasks	"How to Create a Report" on page 1508
See also	➤ "SiteScope Reports Overview" on page 1502 ➤ "Alert Report" on page 1548

Report Targets

User interface elements are described below:

UI Element	Description
Report targets	Displays the groups, monitors, or both, to be included in this report in the context menu tree. The context menu includes the currently selected container and all of the child containers. **Note:** You cannot remove any of the groups or monitors in the selected container from the report.

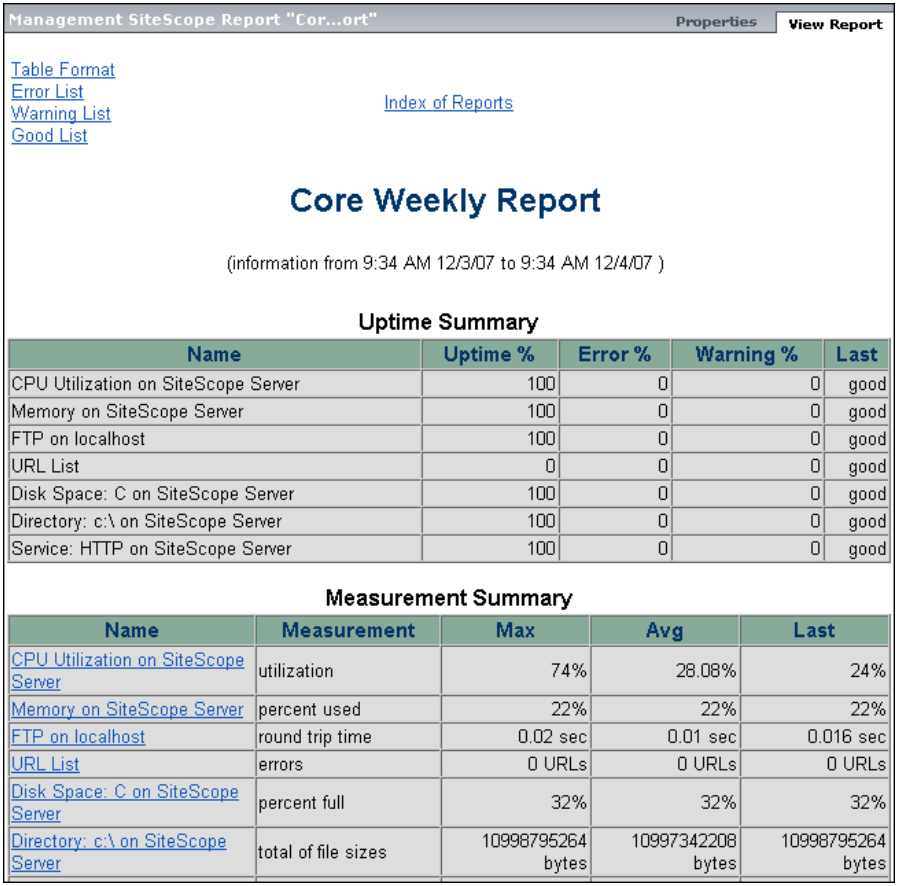
Alert Report Settings

User interface elements are described below:

UI Element	Description
Alert types	Select the alert types that you want to include in the report. **Note:** Hold down the SHIFT key to select a set of adjacent groups. Use CTRL-click to select non-adjacent items.
Detail level	Select the level of detail to include in the report. The options are: ➤ **Basic.** Displays the time and summary information for each alert sent (default setting). ➤ **Detail for all alerts.** Displays detailed alert information for each alert in the report. ➤ **Detail for failed alerts.** Displays the time and summary information for each alert, and a full diagnostics breakdown for each failed alert.
Alert time period	Specify the period of time that you want the report to cover. Select or enter the time and date you want report coverage to start in the **From** boxes and the time and date you want coverage to end in the **To** boxes. **Default value:** The alert time period is from one hour before the time that the Alert Report is generated until the current time. **Note:** Times must be entered in 24-hour format.

Management Report

This report displays a summary and specific details of infrastructure availability and performance data for monitors and monitor groups over a given period of time. Use Management reports to detect emerging trends and correct potential problems before they become a crisis.



Management SiteScope Report "Cor...ort" Properties View Report

Table Format
Error List
Warning List
Good List

Index of Reports

Core Weekly Report

(information from 9:34 AM 12/3/07 to 9:34 AM 12/4/07)

Uptime Summary

Name	Uptime %	Error %	Warning %	Last
CPU Utilization on SiteScope Server	100	0	0	good
Memory on SiteScope Server	100	0	0	good
FTP on localhost	100	0	0	good
URL List	0	0	0	good
Disk Space: C on SiteScope Server	100	0	0	good
Directory: c:\ on SiteScope Server	100	0	0	good
Service: HTTP on SiteScope Server	100	0	0	good

Measurement Summary

Name	Measurement	Max	Avg	Last
CPU Utilization on SiteScope Server	utilization	74%	28.08%	24%
Memory on SiteScope Server	percent used	22%	22%	22%
FTP on localhost	round trip time	0.02 sec	0.01 sec	0.016 sec
URL List	errors	0 URLs	0 URLs	0 URLs
Disk Space: C on SiteScope Server	percent full	32%	32%	32%
Directory: c:\ on SiteScope Server	total of file sizes	10998795264 bytes	10997342208 bytes	10998795264 bytes

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor container, and select **Reports** > **Management**. Configure the report properties, and click **OK**. In the Reports tab, select the report and click the **Generate Report**  button. Click the date-coded link for the report period you want to view. If no reports have been generated, or if you want to create an updated report, click the **Generate** button.
Important information	➤ Management reports do not support non-English labels. ➤ Indicator values are not displayed in SiteScope reports.
Relevant tasks	"How to Create a Report" on page 1508
See also	➤ "Working with SiteScope Management Reports" on page 1506 ➤ "New/Edit SiteScope Management Report Dialog Box" on page 1513 ➤ "Reports Page" on page 1510

Report Content - Index Page

The following elements are included in the Management report index page:

UI Element	Description
Most Recent Report	Click to display the most recent Management report available for the currently selected monitor or group.
Information For <report time and data>	Click to display the Management report for the time period specified in the link for the currently selected monitor or group. For details on the Management Report page, see "Report Content - Management Report Page" below.
Generate	Click to create a new report for the currently selected monitor or group, regardless of when the report was normally scheduled to be generated.

Report Content - Management Report Page

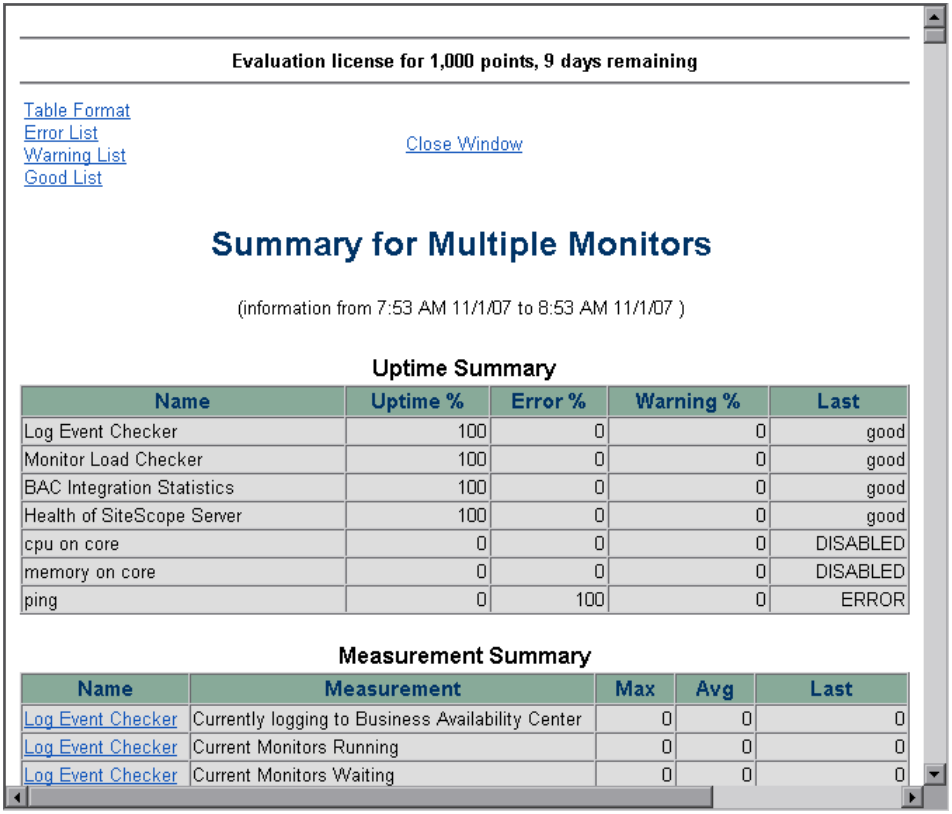
The following elements are included in the Management report page:

UI Element	Description
Table Format	Click the **Table Format** link to go to the measurements data in table format in the currently selected report.
Error List	Click the **Error List** link to go to the list of monitors with error status in the currently selected report.
Warning List	Click the **Warning List** link to go to the list of monitors with warning status in the currently selected report.
Good List	Click the **Good List** link to go to the list of monitors with good status in the currently selected report.
Index of Reports	Click the **Index of Reports** link to go to the index of Management reports. For details on the Management Report index page, see "Report Content - Index Page" on page 1539.
Uptime Summary	This table includes the following: ➤ **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.

UI Element	Description
Measurement Summary	This table includes the following: ➤ **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.
<Measurement Graphs>	Measurement data in graph format for each monitored instance for the report period.
<Measurement Tables>	Measurement data in table format, shown at 30 minute increments, for each monitored instance for the report period. Entries highlighted in red or yellow indicate that the measurement exceeded the error or warning status threshold for the monitor. Blue indicates that the monitor was disabled.
<Error List Table>	Lists the monitor instances that exceeded the error status threshold for the monitor. Entries are highlighted in red.
<Warning List Table>	Lists the monitor instances that exceeded the warning status threshold for the monitor. Entries are highlighted in yellow.
<Good List Table>	Lists the monitor instances that were in the good status threshold for the monitor. Entries are highlighted in green.

Quick Report

This report displays a summary and specific details of infrastructure availability and performance data for monitors and monitor groups over a given period of time. Quick reports are generated on an ad hoc basis and are not saved to the SiteScope configuration data.



Evaluation license for 1,000 points, 9 days remaining

Table Format
Error List
Warning List
Good List

Close Window

Summary for Multiple Monitors

(information from 7:53 AM 11/1/07 to 8:53 AM 11/1/07)

Uptime Summary

Name	Uptime %	Error %	Warning %	Last
Log Event Checker	100	0	0	good
Monitor Load Checker	100	0	0	good
BAC Integration Statistics	100	0	0	good
Health of SiteScope Server	100	0	0	good
cpu on core	0	0	0	DISABLED
memory on core	0	0	0	DISABLED
ping	0	100	0	ERROR

Measurement Summary

Name	Measurement	Max	Avg	Last
Log Event Checker	Currently logging to Business Availability Center	0	0	0
Log Event Checker	Current Monitors Running	0	0	0
Log Event Checker	Current Monitors Waiting	0	0	0

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor container, and select **Reports** > **Quick**. Configure the report properties, and click **Generate Report**. Alternatively, you can create a report using preconfigured settings, by selecting a monitor and clicking the **Quick Report** button in the SiteScope Dashboard toolbar.
Important information	➤ The time interval for a Quick report is not incremented automatically. This means that the report always contains the data for the absolute **Report Period** interval defined in the report definition. To view more recent data using a Quick report, edit the **Report Period** setting. ➤ When working in BSM, Quick Report definitions in SAM Administration are stored only with the BSM context. Quick Report definitions are not stored in and do not persist on the SiteScope server.
Relevant tasks	"How to Create a Report" on page 1508
See also	"New SiteScope Quick Report Dialog Box" on page 1527

Report Content

User interface elements are described below (unlabeled elements are shown in angle brackets):

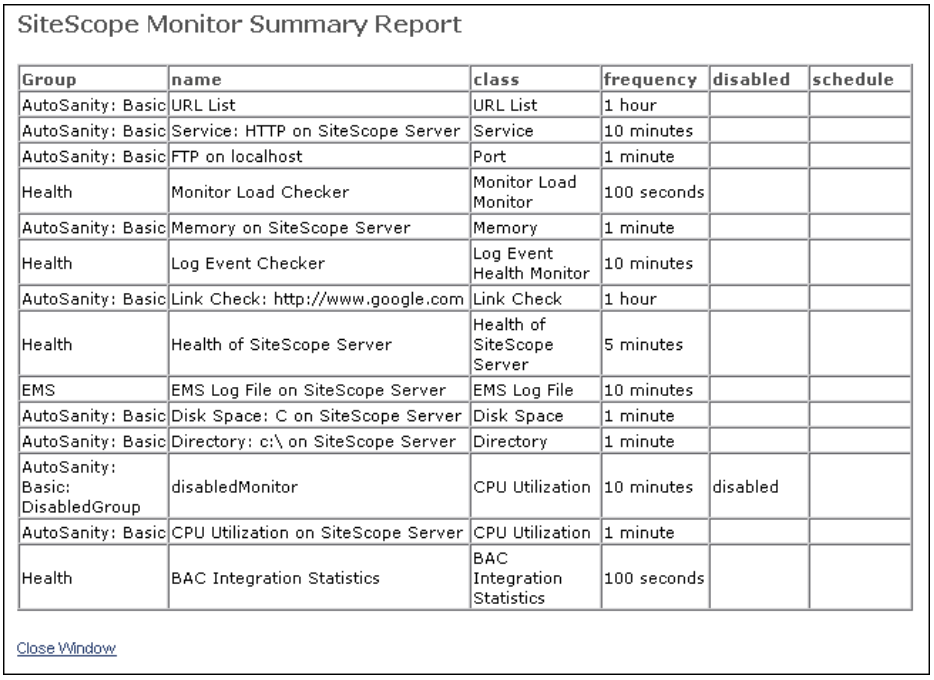
UI Element	Description
<License details>	Displayed when using an evaluation license or a license that has expired. License details are displayed at the top of the page. It includes the SiteScope license category, the number of monitor points available, and the number of days remaining on the license.
Table Format	Click to go to the measurements data in table format in the currently selected report.
Error List	Click to go to the list of monitors with error status in the currently selected report.

UI Element	Description
Warning List	Click to go to the list of monitors with warning status in the currently selected report.
Good List	Click to go to the list of monitors with good status in the currently selected report.
Uptime Summary	This table includes the following: ➤ **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.
Measurement Summary	This table includes the following: ➤ **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.
<Measurement Graphs>	Measurement data in graph format for each monitored instance for the period of the report.

UI Element	Description
<**Measurement Tables**>	Measurement data in table format, shown at 30 minute increments, for each monitored instance for the period of the report. Entries highlighted in red or yellow indicate that the measurement exceeded the error or warning status threshold for the monitor. Blue indicates that the monitor was disabled.
<**Error List Table**>	Lists the monitor instances that exceeded the error status threshold for the monitor. Entries are highlighted in red.
<**Warning List Table**>	Lists the monitor instances that exceeded the warning status threshold for the monitor. Entries are highlighted in yellow.
<**Good List Table**>	Lists the monitor instances that were in the good status threshold for the monitor. Entries are highlighted in green.

Monitor Summary Report

This report displays information about the configuration and current settings of monitors in the groups you have selected to include in the report. Use this report to view setup information on monitors as well as the organization and makeup of groups of monitors. For example, you can check and compare monitor run frequencies (the **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.



SiteScope Monitor Summary Report

Group	name	class	frequency	disabled	schedule
AutoSanity: Basic	URL List	URL List	1 hour		
AutoSanity: Basic	Service: HTTP on SiteScope Server	Service	10 minutes		
AutoSanity: Basic	FTP on localhost	Port	1 minute		
Health	Monitor Load Checker	Monitor Load Monitor	100 seconds		
AutoSanity: Basic	Memory on SiteScope Server	Memory	1 minute		
Health	Log Event Checker	Log Event Health Monitor	10 minutes		
AutoSanity: Basic	Link Check: http://www.google.com	Link Check	1 hour		
Health	Health of SiteScope Server	Health of SiteScope Server	5 minutes		
EMS	EMS Log File on SiteScope Server	EMS Log File	10 minutes		
AutoSanity: Basic	Disk Space: C on SiteScope Server	Disk Space	1 minute		
AutoSanity: Basic	Directory: c:\ on SiteScope Server	Directory	1 minute		
AutoSanity: Basic: DisabledGroup	disabledMonitor	CPU Utilization	10 minutes	disabled	
AutoSanity: Basic	CPU Utilization on SiteScope Server	CPU Utilization	1 minute		
Health	BAC Integration Statistics	BAC Integration Statistics	100 seconds		

Close Window

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor container, and select **Reports** > **Monitor**. Configure the report properties, and click **Generate Report**.
Relevant tasks	"How to Create a Report" on page 1508
See also	"New SiteScope Monitor Report Dialog Box" on page 1533

Report Content

User interface elements are described below:

UI Element	Description
Group	The group name to which the monitor belongs.
Name	The display name or text description for each monitor.
Class	The monitor type.
Frequency	The frequency at which the monitor is set to run.
Disabled	Indicates whether the monitor is disabled.
Depends on	Lists any dependent monitors, if the running of this monitor is dependent on the status of other monitors.
Points	The number of license points used by the monitor instance.
OID	The Object ID for this monitor.
Schedule	The monitor schedule, if a schedule other than the default schedule is selected.
Error Frequency	If the **Error frequency** option is selected, the monitoring interval, in seconds, for monitors that have reported an error condition.
Timeout	The timeout setting for the monitor.
Verify Error	Displays On if the **Verify error** option is selected. This option automatically runs the monitor again if it detects an error.
Monitor Description	The text description for the monitor in the Monitor Description box.
Thresholds	The threshold conditions for the monitor instance.

Alert Report

This report displays information about SiteScope alerts generated during a specified period of time for the monitors in the selected container.

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

To access	Select the **Monitors** context. In the monitor tree, right-click the SiteScope node, a monitor group, or a monitor container, and select **Reports** > **Alert**. Configure the report properties, and click **Generate Report**.
Relevant tasks	"How to Create a Report" on page 1508
See also	"New SiteScope Alert Report Dialog Box" on page 1536

Report Content

User interface elements are described below:

UI Element	Description
<Report title>	The report title contains the name of the monitor group container or individual monitor for which the report was created, and the time period that the report covers.
Time	The time at which the alert was triggered.
Type	The type of alert action.
Message	The type of message in the alert (for example, Default, alarm).
Monitor	The name of the monitor on which the alert was triggered.
Group	The name of the group on which the alert was triggered.

Annotation Tool

This tool enables you to annotate a snapshot of the report you are viewing, to highlight important areas. The Annotation Tool is available when viewing Baseline Monitor Measurements Graphs. The Annotation Options enable you to customize your snapshot.

The Annotation Menu Bar contains elements that enable you to:

- Change the appearance of the snapshot.
- Save, print, or email an annotation report.
- Customize the appearance of text annotated onto your snapshot. These elements are enabled only when the Text Tool T button is selected.

To access	Click the **Annotate** button on the right side of the page.
Important information	To use the Annotation Tool, the Sun JRE plug-in 1.6.0_x (latest version recommended) must be installed on your machine. If the plug-in is not installed on your machine, you are prompted to install it.
See also	"Setting Status Thresholds Using a Baseline" on page 405

Annotation Options

User interface elements are described below:

UI Element (A–Z)	Description
	**Pan Tool.** Click to navigate the snapshot.
	**Select Tool.** Click to select a specific area of the snapshot.

UI Element (A–Z)	Description
	**Shape Tool.** Click to add a shape to the snapshot. Clicking the shape tool button enables the following shape buttons: ➤  **Rectangle.** Click to mark an area of the snapshot with a rectangle. ➤  **Filled Rectangle.** Click to mark an area of the snapshot with a filled rectangle. ➤  **Oval.** Click to mark an area of the snapshot with an oval. ➤  **Filled Oval.** Click to mark an area of the snapshot with a filled oval. ➤  **Rounded Rectangle.** Click to mark an area of the snapshot with a round rectangle. ➤  **Filled Rounded Rectangle.** Click to mark an area of the snapshot with a filled round rectangle. **Customization.** After selecting this button, you can customize your line appearance through the following parts of the interface: ➤ **Line Type.** Choose the type of line you want to add. Options include: ➤ Solid Line ➤ Jagged Line ➤ **Line Width.** Select the width of the line, in pixels, in the annotation.

UI Element (A–Z)	Description
	**Line Tool.** Click to enable the line tool, which marks the selected area of the snapshot with a line. **Customization.** After selecting this button, you can customize your line appearance through the following parts of the interface: ➤ **Line Style.** Choose the style of line you want to add. Options include: ➤ Regular line ➤ Line with endpoints ➤ Line with arrows ➤ **Line Type.** Choose the type of line you want to add. Options include: ➤ Solid Line ➤ Jagged Line ➤ **Line Width.** Select the width of the line, in pixels, in the annotation.
	**Text Tool.** Click to add text to the snapshot. **Example:** Add the syntax This is the problematic transaction above a line marking an area of the report.

UI Element (A–Z)	Description
Border and Fill Colors	Select the relevant square to choose the color of the border and fill of your annotations. The available squares are: ➤ **Upper Square.** Click to choose the color of lines, as generated by the line tool and displayed in unfilled shapes. ➤ **Lower Square.** Click to choose the color to fill shapes. Clicking either of the squares generates a dialog box with the following tabs where you choose the color: ➤ Swatches ➤ HSB ➤ RGB
Opacity	Slide the opacity bar to choose the darkness level of the selected shape line, text line, or shape color in the annotation. **Note:** ➤ A higher opacity percentage means that the selection appears darker. A lower opacity percentage means that the selection appears lighter. ➤ This field is enabled when either the shape tool, line tool, or text tool button is selected.

Annotation Menu Bar

User interface elements are described below:

UI Element (A–Z)	Description
	**Save.** Saves the snapshot on your local machine. **Note:** ➤ The snapshot is saved in .png format. ➤ You cannot select the **New Folder** icon  when saving in the **My Documents** directory or any of its subdirectories.
	**Select All.** Selects all of the annotations added to your snapshot.
	**Clear Selected.** Clears all annotations.
	**Undo.** Rolls back the most recent action performed on the snapshot.
	**Redo.** Cancels the roll back of the most recent action performed on the snapshot.
	**Zoom In.** Brings the snapshot view closer.
	**Zoom Out.** Sets the snapshot view further away.
	**Restore original size.** Restores the snapshot to its original size.
	**Print.** Prints the snapshot.
	**Send E-mail.** Click to send the snapshot via email.
	**Save to repository.** Uploads the snapshot to the Report Manager. For details on the Report Manager, see "Report Manager Overview" on page 28. **Note:** This option is not available when accessing the Annotation Tool from the SiteScope feature.

UI Element (A–Z)	Description
	**Help.** Displays online documentation help for the page you are currently viewing.
	**Bold.** Bolds the text. **Note:** This field is enabled only when selecting the **Text Tool** button  .
	**Italic.** Italicizes the text. **Note:** This field is enabled only when selecting the **Text Tool** button  .
	**Underline.** Underlines the text. **Note:** This field is enabled only when selecting the **Text Tool** button  .
	**Anti-aliasing.** Adjusts the pixel reading of text or annotation lines so that they appear smoother. **Note:** This field is only enabled when selecting the **Text Tool** button  .
<Font Family>	Select the font for the text in the report. **Note:** This field is only enabled when selecting the **Text Tool** button  .
<Font Size>	Select the size of the font in the report. **Note:** This field is only enabled when selecting the **Text Tool** button  .

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X