OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

Managing SiteScope

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

Managing SiteScope

Version 6.1

Document Release Date: February 15, 2006

MERCURY™

Mercury Business Availability Center, Version 6.1
Managing SiteScope

This manual, and the accompanying software and other documentation, is protected by U.S. and international copyright laws, and may be used only in accordance with the accompanying license agreement. Features of the software, and of other products and services of Mercury Interactive Corporation, may be covered by one or more of the following patents: United States: 5,511,185; 5,657,438; 5,701,139; 5,870,559; 5,958,008; 5,974,572; 6,137,782; 6,138,157; 6,144,962; 6,205,122; 6,237,006; 6,341,310; 6,360,332, 6,449,739; 6,470,383; 6,477,483; 6,549,944; 6,560,564; 6,564,342; 6,587,969; 6,631,408; 6,631,411; 6,633,912; 6,694,288; 6,738,813; 6,738,933; 6,754,701; 6,792,460 and 6,810,494. Australia: 763468 and 762554. Other patents pending. All rights reserved.

Mercury, Mercury Interactive, the Mercury logo, the Mercury Interactive logo, LoadRunner, WinRunner, SiteScope and TestDirector are trademarks of Mercury Interactive Corporation and may be registered in certain jurisdictions. The absence of a trademark from this list does not constitute a waiver of Mercury's intellectual property rights concerning that trademark.

All other company, brand and product names may be trademarks or registered trademarks of their respective holders. Mercury disclaims any responsibility for specifying which marks are owned by which companies or which organizations.

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

Mercury Interactive Corporation
379 North Whisman Road
Mountain View, CA 94043
Tel: (650) 603-5200
Toll Free: (800) TEST-911
Customer Support: (877) TEST-HLP
Fax: (650) 603-5300

© 2006 Mercury Interactive Corporation, All rights reserved

If you have any comments or suggestions regarding this document, please send them by e-mail to documentation@mercury.com.

AMLIB_MANSIS6.1/01

Table of Contents

Welcome to Managing SiteScope vii
How This Guide Is Organized vii
Who Should Read This Guide viii
Getting More Information viii

PART I: MANAGING SITESCOPE IN THE MONITOR TREE

Chapter 1: Managing SiteScope in the Monitor Tree 3
About Working with SiteScopes in the Monitor Tree 3
Integrating SiteScope with Mercury Business Availability Center 5
SiteScope Profile Integration Status 6
Adding a SiteScope to Monitor Administration and Defining SiteScope Settings 9
Adding Groups to a SiteScope 14
Managing SiteScope Monitors 15
Replicating Configuration Settings 19
Removing a SiteScope from Monitor Administration 20

PART II: SITESCOPE PREFERENCES

Chapter 2: Introducing SiteScope Preferences 25
Preferences Overview 25

Chapter 3: Absolute Schedule Preferences 29
Working with Absolute Schedules 29
Absolute Schedule Settings 32

Chapter 4: SiteScope General Preferences 33
Configuring General Preferences Properties 33
Working in an I18N Environment 36
Using Default Authentication Credentials 38
Suspending Monitor Processes 39
Working with SiteScope Configuration Files 40

Chapter 5: Logging Preferences 43
Understanding SiteScope Logs and Data Logging Options 43
Setting SiteScope Log Preferences 44
Troubleshooting Database Connections 46
SiteScope Log Database Table Structure 48

Chapter 6: E-mail Preferences 51
Working with SiteScope E-mail Preferences 51
Configuring E-mail Preferences Properties 52
Working with E-mail Recipient Profiles 54
E-mail Recipient Profile Settings 56

Chapter 7: Pager Preferences 59
Working with SiteScope Pager Preferences 59
Configuring Pager Preferences Properties 60
Working with Pager Recipient Profiles 64
Pager Recipient Profile Settings 66

Chapter 8: Range Schedule Preferences 69
Working with Range Schedules 69
Range Schedule Settings 72

Chapter 9: SNMP Trap Preferences 75
Working with SiteScope SNMP Trap Preferences 75
Configuring SNMP Trap Preferences Properties 76
Working with SNMP Trap Profiles 77
SNMP Trap Profile Settings 79

Chapter 10: UNIX Remote Preferences 81
Monitoring Remote UNIX Servers 81
Unix Server Profile Settings 83
Technical Notes on Remote UNIX Monitoring 89

Chapter 11: Windows Remote Preferences 93
Monitoring Remote Windows Servers 93
Windows Server Profile Settings 96
Technical Notes on Remote Windows Monitoring 100

PART III: SITESCOPE HEALTH

Chapter 12: Monitoring SiteScope Server Health 107
About the SiteScope Health Group 107
Adding SiteScope Health Monitors 108
Understanding SiteScope Health Monitoring 109

Chapter 13: SiteScope Health Monitor Reference 113
Log Event Health Monitor 113
Monitor Load Monitor 115
Health of SiteScope Server Monitor 116

Chapter 14: SiteScope Logs 121

Index 125

Welcome to Managing SiteScope

This guide provides instructions on how to manage SiteScope within the monitor tree in Monitor Administration. This includes adding, deleting, detaching, and attaching a SiteScope to the monitor tree. This guide also describes creating groups, defining settings, configuring preferences, and setting up the SiteScope heath templates for self monitoring.

How This Guide Is Organized

The guide contains the following chapters:

Part I Managing SiteScope in the Monitor Tree

Describes how to work with SiteScope monitor groups and optional preferences and settings.

Part II SiteScope Preferences

Describes how to configure SiteScope preference options for how to connect to remote servers, e-mail server, logging of monitor measurement data, and other settings.

Part III SiteScope Health

Describes how to configure and interpret SiteScope self-monitoring.

Who Should Read This Guide

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

- Mercury Business Availability Center administrators
- Mercury Business Availability Center data collector administrators

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.

Getting More Information

For information on using and updating the Mercury Business Availability Center Documentation Library, reference information on additional documentation resources, typographical conventions used in the Documentation Library, and quick reference information on deploying, administering, and using Mercury Business Availability Center, refer to *Getting Started with Mercury Business Availability Center*.

Part I

Managing SiteScope in the Monitor Tree

1

Managing SiteScope in the Monitor Tree

You can configure multiple SiteScopes using Monitor Administration. The console's monitor tree displays containers for physical SiteScopes and their associated preference configurations, groups, subgroups, monitors, and alerts.

This chapter describes:	On page:
About Working with SiteScopes in the Monitor Tree	3
Integrating SiteScope with Mercury Business Availability Center	5
SiteScope Profile Integration Status	6
Adding Groups to a SiteScope	14
Managing SiteScope Monitors	15
Replicating Configuration Settings	19
Removing a SiteScope from Monitor Administration	20

About Working with SiteScopes in the Monitor Tree

Monitor Administration enables you to:

- add a SiteScope to Monitor Administration and edit a SiteScope's settings (for details, see "SiteScope Profile Integration Status" on page 6)
- add groups and subgroups (for details, see "Adding Groups to a SiteScope" on page 14)
- copy and paste configuration settings for groups, monitors, and alerts (for details, see "Replicating Configuration Settings" on page 19)

- detach or delete a SiteScope from Monitor Administration (for details, see "Removing a SiteScope from Monitor Administration" on page 20)
- configure SiteScope monitors (for details, see "Managing SiteScope Monitors" on page 15)

You use the monitor tree to navigate through containers and elements in the tree structure and drill down to monitor and other configuration settings. For details on the different hierarchy elements, see "Using Monitor Administration" in *Working with Monitor Administration*

You can customize your view of the monitor tree to list only those SiteScope elements with which you are working. You can also assign categories to your SiteScopes, groups, monitors, and alerts to further refine your selection. For details, see "Setting Views and Defining Categories" in *Working with Monitor Administration*.

Monitor Administration enables you to change monitor configurations across multiple monitors, groups, or multiple SiteScopes using Global Replace. For details, see "Using Global Replace" in *Working with Monitor Administration*.

You can also use templates to speed the monitor deployment of a single SiteScope or replicate group and monitor hierarchies across multiple SiteScopes. For details, see "Using Templates to Deploy Monitors" in *Configuring SiteScope Monitors*.

Several pre-defined templates, called solution templates, are available for deployment within the monitor tree. The availability of these solution templates depends on your SiteScope license. For details, see "Introducing SiteScope Solution Templates" in *Configuring SiteScope Monitors*.

Integrating SiteScope with Mercury Business Availability Center

There are three options for integrating SiteScope into Mercury Business Availability Center.

- You can import the SiteScope into Monitor Administration to enable both configuration within Monitor Administration and reporting SiteScope data to Mercury Business Availability Center applications.

  To enable both reporting to Mercury Business Availability Center and configuration in Monitor Administration, select **Import SiteScope Configuration** and select **Enable Reporting to Mercury Business Availability Center** in step 6 of "SiteScope Profile Integration Status" on page 6.

- You can enable the reporting of SiteScope data to Mercury Business Availability Center while configuring the SiteScope on the SiteScope server using the SiteScope interface without transferring control of the SiteScope to Monitor Administration.

  To enable this scenario, you must create an empty SiteScope profile by adding the SiteScope to Monitor Administration. While adding the SiteScope, clear **Import SiteScope Configuration** and select **Enable Reporting to Mercury Business Availability Center** in step 6 of "SiteScope Profile Integration Status" on page 6.

- You can configure multiple SiteScopes using Monitor Administration without enabling the reporting of SiteScope data to Mercury Business Availability Center.

  To enable this scenario, while adding the SiteScope to Monitor Administration, select **Import SiteScope Configuration** and clear **Enable Reporting to Mercury Business Availability Center** in step 6 of "SiteScope Profile Integration Status" on page 6.

SiteScope Profile Integration Status

Once a SiteScope is added to the monitor tree in Monitor Administration, the name of each SiteScope profile appearing in the tree is followed by its integration status in parentheses. The exception is attached status where the profile appears without the status in parenthesis. The status is automatically updated to reflect user operations on the profile within Monitor Administration and within SiteScope.

The possible statuses for a SiteScope in the monitor tree are **New**, **Registered**, **Attached**, **Detached**, are **Reset**.

Understanding Integration Status

Below is a description of each integration status:

- **New** – A profile created in Monitor Administration with no imported configuration. The profile's configuration is empty in the Monitor Administration tree. This status is assigned while the SiteScope profile is being created in Monitor Administration before it is registered to Mercury Business Availability Center. It is usually a temporary status.
- **Registered** – A profile whose configuration has never been imported. The profile's configuration is empty in the Monitor Administration tree. This SiteScope sends data to Mercury Business Availability Center applications but is not controlled by Monitor Administration. Configuration must be done directly on the SiteScope server.
- **Attached** – A profile registered to Mercury Business Availability Center and controlled by Monitor Administration. The configuration from the SiteScope server is imported to Monitor Administration and the SiteScope object appears in the monitor tree with all its child objects and is configurable only within Monitor Administration. This status is not displayed in the monitor tree. Any SiteScope profile that is attached is displayed with its profile name only.
- **Detached** – A profile that was attached at least once but is not currently attached to Monitor Administration. Configuration is controlled by the SiteScope server itself. The profile's configuration is empty in the monitor tree. The SiteScope continues to report data to Mercury Business Availability Center applications.

➤ **Reset** – A profile whose integration was reset from SiteScope by a SiteScope user. The profile remains in Mercury Business Availability Center and can be used to prepare history reports. Data, however, is not reported to Mercury Business Availability Center applications. The profile cannot be controlled from Monitor Administration. The profile's configuration is empty in the monitor tree.

Disabling/Enabling the Profile Status Feature

The profile status feature can be disabled in either Mercury Business Availability Center or by modifying the SiteScope configuration file. Once the feature is disabled, the status does not appear beside the SiteScope profile name in the monitor tree.

Disabling the feature only in Mercury Business Availability Center is enough to disable the feature. If, however, you want to disable specific SiteScopes connected to the same Mercury Business Availability Center installation, but not all, it is recommended to keep the feature enabled in Mercury Business Availability Center and disable the feature in the individual SiteScope configuration file.

To disable the profile status feature in Mercury Business Availability Center:

1. Click **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings.** The Infrastructure Settings page opens.
2. Select **Foundations** and select **SiteScope Events** from the list of applications.
3. Click the **Edit** button.
4. Select **false** to disable the status feature. The change takes effect immediately.

Note: Select **true** to enable the profile status feature.

To disable the profile status feature in a specific SiteScope's configuration file:

1 Edit **<SiteScope_install_path>\groups\master.config** file. Set the following variables:

- **_topaz_status_checker_enable=false.** Disables sending SiteScope status changes.
- **_topaz_status_checker_enable_schedule=false.** Disables the ability to schedule status checks. When disabled, **_topaz_status_check_time_interval** is also automatically disabled.

2 Restart SiteScope.

Note:

To enable the profile status feature on the SiteScope side, do the following:

- Set **_topaz_status_checker_enable= true**.
- Set **_topaz_status_checker_enable_schedule=true**.
- Set **_topaz_status_check_time_interval** to the frequency of status checks in minutes. The minimum frequency is 1 (minute). The default is 5 (minutes). The default value is used if **_topaz_status_check_time_interval** is undefined or defined incorrectly.
- Restart SiteScope.

Known Limitations

There are several limitations:

- Operations affecting the integration between SiteScope and Monitor Administration done in SiteScope are reflected in the status displayed in Monitor Administration only if there is network communication between SiteScope and Mercury Business Availability Center.
- Performing a synchronization in Monitor Administration may temporarily remove the integration status. The next scheduled update of SiteScope status corrects the status in the LDAP and in Monitor Administration.

- While editing a SiteScope profile, the status text itself can also be edited. It is strongly recommended, however, not to manually change the status text in the parentheses as this may damage the profile. You can edit the display name that appears to the left of the status.
- Only SiteScope profiles with **Attached** status can be controlled by Monitor Administration. In all statuses other than **Attached**, the SiteScope profile in the monitor tree appears empty. If you want to configure the SiteScope within Mercury Business Availability Center, you must first attach the profile or select to import configurations when creating the profile.

Adding a SiteScope to Monitor Administration and Defining SiteScope Settings

The SiteScope tree object represents one physical SiteScope. A SiteScope can be added or imported directly to the enterprise node or into any user-defined container. For details on containers, see "Using Monitor Administration" in *Working with Monitor Administration*.

To enable Mercury Business Availability Center to receive the data that SiteScope collects, the SiteScope must be associated with a SiteScope profile and be registered to report to Mercury Business Availability Center. Monitor Administration enables you to define profiles and to directly access the SiteScope interface for performing the necessary verification and registration procedures.

When you add a SiteScope to Mercury Business Availability Center's Monitor Administration:

- SiteScope group, monitor, alert, and preference settings are copied to Monitor Administration.
- Add and edit privileges are suspended for any user accessing the SiteScope from outside Monitor Administration for as long as it is attached to the console.

To add a SiteScope to Monitor Administration:

1 Access Monitor Administration from Mercury Business Availability Center (**Admin** > **Monitors**).

2 Select from the following options:

- In the monitor tree, right-click the enterprise node or user-defined container into which you want to add a new SiteScope and select **New SiteScope** in the container's menu.
- In the **Contents** tab, click the **New SiteScope** button at the top of the page.

The **Add SiteScope** page opens.

3 In the **Main Settings** area:

- Enter a descriptive name representing this SiteScope in the tree in the **SiteScope Name** box. This name identifies the SiteScope while it is attached to Monitor Administration.
- Enter the host name or IP address of the machine on which SiteScope is currently running in the **Host Name** box.
- Enter the port number used to communicate with SiteScope in the **Port Number** box. The default value is 8888.
- Select **Use SSL** to secure the communication of the SiteScope API through a secure HTTPS.

4 In the **Distributed Settings** area:

- Enter the name or IP address of the Core Server in the **Core Machine name/IP address** box only if the Core Server is installed on a different machine than the Centers Server. If no value is entered, the default is used.
- Enter the SiteScope agent machine location in the **SiteScope agent machine location** box. The default is used if no value is entered.
- Enter the login user name of the Core Server in the **Core Machine Authentication username** box. The default is used if no value is entered.
- Enter the login password of the Core Server in the **Core Machine Authentication password** box. The default is used if no value is entered.

5 In the **Advanced Settings** area:

- ➤ Enter the SiteScope account name needed to connect with SiteScope in the **SiteScope Account Name** box. The default is the administrator account name. To determine the account name, see the login URL in the SiteScope User Preference settings. Typically, it is administrator or login1.
- ➤ Enter the SiteScope login name in the **SiteScope Login Name** box. The default is the administrator login name.
- ➤ Enter the SiteScope login password in the **Password** box if the SiteScope you are adding has been set up with a password.
- ➤ The following values are automatically imported from the SiteScope you are adding and the fields are not editable:
  - **SiteScope Version**
  - **Build Time**, **Build Date**, and **Build Number**
  - **Platform**
  - **OS** (operating system)
  - **OS Version** (version of operating system)
- ➤ Enter a description for this SiteScope in the **Description** box.

6 In the **Profile Settings** area, define the following properties to establish a profile for this SiteScope, enabling the data collected by the SiteScope to be reported to Mercury Business Availability Center and the profile database:

- ➤ Select **Import SiteScope Configuration** to import to Mercury Business Availability Center all the data related to the SiteScope and to enable Monitor Administration to control the SiteScope while it is attached.

  Clear **Import SiteScope Configuration** to add the SiteScope to the monitor tree without its data and without the ability to control the SiteScope in Monitor Administration.
- ➤ Enter the profile name in the **Profile Name** box. The SiteScope name is used if no value is entered. The name serves as an identifier of the profile for management operations and reports.

Tip: Include the name of the SiteScope in the profile name to be able to identify the SiteScope while accessing reports.

- Select the GMT Offset for the SiteScope profile used for reports and aggregation purposes in the **GMT Offset** list. For a list of GMT time zones, see "GMT Time Zones" in *Reference Information*.
- Select the database (MS SQL) or schema (Oracle) into which the profile information is saved in the **Database Schema** list.
- Enter the user name for the authentication (basic authentication and protocol) of the Web server security options in the **Webserver Authentication username** box.
- Enter the password for the authentication of the Web server security options (basic authentication and protocol) in the **Webserver Authentication password** box.
- Select **Use SSL (HTTPS) protocol** for the Web server to use http protocol over a secure connection.
- In the **Proxy name/IP Address** box, enter values if SiteScope uses a proxy to connect to the Mercury Business Availability Center server.
- Enter the user name for logging into the proxy server in the **Proxy Username** box.
- Enter the password for logging into the proxy server in the **Proxy Password** box.
- Select **Enable Reporting to Mercury Business Availability Center** to enable reporting SiteScope measurements to Mercury Business Availability Center.
- Select **Resync SiteScope with Mercury Business Availability Center** to resynchronize SiteScope data with Mercury Business Availability Center data.

7 Optionally, if there are any categories defined, you can assign a category to the SiteScope under the **Category Settings** section.

For details on defining categories, see "Working with Categories" in *Working with Monitor Administration*.

8 Click **Add**.

Importing SiteScope data may take some time depending on the number of monitors that are configured and running on the SiteScope machine. When the import is finished, a SiteScope container is added to the monitor tree using the name entered in the **SiteScope** field.

Editing SiteScope Settings

SiteScope settings include the host name, port number, and login information for accessing the SiteScope. You may need to edit these configurations over time. For example, Monitor Administration communicates with remote SiteScopes using the HTTP protocol. If the port number on which the SiteScope server is running changes, you have to update the SiteScope settings in Monitor Administration.

To edit SiteScope settings:

1 In Monitor Administration, access the Edit SiteScope page. For details, see "Accessing Object Properties for Editing" in *Working with Monitor Administration*.

2 Edit the **SiteScope** properties as required.

3 Click **OK**. The SiteScope is updated in the monitor tree.

Adding Groups to a SiteScope

SiteScope monitors are organized into groups. Monitor groups are displayed as a node in the SiteScope container or in a group container in Monitor Administration.

Note: If you want to add a SiteScope monitor, your SiteScope must include at least one group container.

Use the following steps to add a new group to a SiteScope or a new subgroup to an existing SiteScope group.

To add a SiteScope group or subgroup:

1 In Monitor Administration, select from the following options:

- In the monitor tree, right-click the SiteScope container into which you want to add a new group or the group into which you want to add a subgroup and choose **New Group** in the object's menu.
- In the **Contents** tab with the SiteScope highlighted in the monitor tree, click the **New Group** button at the top of the page.

The **New SiteScope Group** page opens.

2 In the **Main Settings** section, enter a name for the group you are creating in the **Group Name** box.

Note: The name of the SiteScope group must contain at least one alphanumeric character at the start of the name, for example a-z, A-Z, 0-9.

---

3 Expand the **Advanced Settings** options to add a refresh schedule, custom description, or specify a group dependency for this group.

4 If required, enter a description in the **Group Description** box.

5 If you are creating an enable/disable dependency between this group and some other monitor instance on this SiteScope, select that monitor as the primary monitor in the **Depends On** list.

Use the drop-down list to select from all the available groups and monitors that can be used to build the dependency.

6 If you are creating a dependency condition, select the condition for the primary monitor or group in the **Depends Condition** list.

The conditions are:

- **OK –** the monitors in the group are enabled and run as long as the primary monitor reports an **OK** status. This is the default option.
- **Error** - if the primary monitor is in an error state, the monitors in the group will be disabled.

7 Optionally, if there are any categories defined, you can assign a category to the SiteScope group under the **Category Settings** section.

For details on defining categories, see "Working with Categories" in *Working with Monitor Administration*.

8 Click **Add**. The new group is added to the monitor tree.

Managing SiteScope Monitors

Monitor Administration enables you to add SiteScope monitors to your enterprise and to centrally manage all those monitors. When adding a monitor, you select the type of monitor and then define the specific parameters for the monitor instance you are creating. You can create another instance of that monitor type and enter different monitoring parameters.

You can also enable and disable a monitor in the properties page for the monitor.

Adding SiteScope Monitors to the Monitor Tree

SiteScope monitors can be added only to a SiteScope group container and not to any other object within the SiteScope object or the monitor tree. For details on all the available monitor types and how to configure them, see "Working with SiteScope Monitors" in *Configuring SiteScope Monitors*.

To add a new SiteScope monitor to a SiteScope group:

1 Select from the following options:

- In the monitor tree, right-click the SiteScope group to which you want to add a monitor. Select **New Monitor** from the menu. The Add Monitor screen opens.
- Highlight the SiteScope group into which you want to add a monitor. Click **New Monitor** in the Contents tab. The Add Monitor screen opens.

2 Select the monitor from the alphabetical list as shown or scroll down and view the monitors by category.

3 Click the type of monitor you want to add. The applicable Add Monitor screen opens.

4 Enter the configuration settings for the monitor.

The **Main**, **Advanced**, and **Threshold Settings** vary from one monitor type to another. For more detailed information about a particular monitor type's settings, see "SiteScope Monitors" in *Configuring SiteScope Monitors*.

5 Under **Enable/Disable Monitor**, enable or disable the monitor as required. For details, see "Disabling and Enabling Monitors" on page 17.

6 Under **Enable/Disable Alerts**, enable or disable the alerts associated with this monitor as required. For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

7 Under **Mercury BAC Logging**, select an option:

- **Do not report to Mercury Business Availability Center**
- **Report everything (all monitors and all measurements)** – This option sends all monitor data to Mercury Business Availability Center for each time that the monitor runs. This option enables the largest data transfer load.

- **Report monitor level data (no measurements)** – This option 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.
- **Report monitor level data and measurements with thresholds** – This option sends monitor category (error, warning, good), status string, as well as performance counter data for any counters that have been set with thresholds (for example, Error If, Warning If). The data is sent for each time that the monitor is run.
- **Report status changes (no measurements)** – This option sends only monitor category (error, warning, good), status string, and other basic data only when the monitor reports a change in status. No information on specific performance counters is included. This option enables the smallest data transfer load.

8 Optionally, if there are any categories defined, you can assign a category to the monitor under the **Category Settings** section.

For details on defining categories, see "Working with Categories" in *Working with Monitor Administration*.

9 Click **Add**. The monitor is added to the monitor tree. Mercury Business Availability Center transmits the configuration data to the applicable SiteScope.

Disabling and Enabling Monitors

You can disable and enable monitors manually or specify a time period to disable a monitor, after which it is automatically re-enabled. This feature is useful for when you know that the monitors will be in error, such as during routine maintenance or a prolonged outage. Disabling monitors prevents alerts from being generated for those monitors.

Note: You can enable or disable multiple monitors, including monitor groups, using Global Replace. For details, see "Using Global Replace" in *Working with the SiteScope Interface*.

To enable a monitor:

1. While you are configuring or editing the monitor, expand the **Enable/Disable Monitor** area. (For details on accessing a monitor for editing, see "Accessing Object Properties for Editing" in *Working with Monitor Administration*.)
2. Select **Enable Monitor**. When configuring a new monitor, this option is selected by default.

To disable a monitor:

1. While you are configuring or editing the monitor, expand the **Enable/Disable Monitor** area. (For details on accessing a monitor for editing, see "Accessing Object Properties for Editing" in *Working with Monitor Administration*.)
2. Select one of the following options:
   - **Disable Monitor indefinitely** – To re-enable the monitor if this option is selected, you must manually enable the monitor by returning to this page and selecting **Enable Monitor**.
   - **Disable Monitor for the next** – Enter a time period for which the monitor should remain disabled. Select minutes, hours, or days as applicable. If you select this option and leave the time value blank, the monitor remains disabled until it is manually re-enabled.
   - **Disable on a one-time schedule** – Enter a start time and an end time in the following format: 12:00 8/2/2004. The monitor is disabled for the time period specified and automatically re-enabled at the end date and time specified.
3. Enter an optional **Disable Description** in the field indicated. This description appears as part of the monitor status in the group detail page and can include information as to why the monitor is disabled, for example: scheduled maintenance or holiday weekend.

Replicating Configuration Settings

Monitor Administration enables you to define new SiteScope groups, monitors, alerts, and preferences by replicating existing objects with similar configurations. Using a copy/paste procedure, you can define any SiteScope object.

Note: You cannot copy any SiteScope object from a SiteScope running on a Windows platform onto a SiteScope running on a Unix platform, and vice versa.

To copy and paste settings for a SiteScope object:

1 In Monitor Administration, select from the following options:

- In the monitor tree, right-click the group, monitor, or alert that you want to replicate and select **Copy**.
-  In the Contents tab for the group, monitor, or alert action, click the **Copy** button at the top of the page.

The message in the info area indicates whether the copy has been successful.

2 Right-click the monitor tree container into which you want to paste the configuration settings and select **Paste** from the action menu.

- You can paste a monitor's configurations only into a SiteScope group.
- You can paste a group only into a SiteScope, group, or subgroup.
- You can paste an alert only into the same type of container from which you copied it. For example, if you copied the alert from a group container, you paste it into another group or subgroup.

The group, monitor, or alert appears in the monitor tree with duplicated configuration settings.

3 To edit the name or any other settings, right-click the item in the monitor tree and select **Edit** or click the **Edit** button in the Contents tab.

Removing a SiteScope from Monitor Administration

There are two ways in which you can remove a SiteScope from the monitor tree and Monitor Administration, delete the SiteScope or detach the SiteScope.

When you detach a SiteScope from Monitor Administration, the SiteScope continues reporting data to the Mercury Business Availability Center platform and continues to appear in the monitor tree.

When you delete a SiteScope (or a container that contains a SiteScope), the SiteScope is deleted from the monitor tree and no longer reports any data to Mercury Business Availability Center.

When you delete or detach a SiteScope, you:

- discontinue Monitor Administration control over the SiteScope server
- return add and edit privileges to users accessing that SiteScope through the native SiteScope interface

---

Note: A SiteScope, or any container that has a SiteScope as a child element, cannot be copied and pasted to another branch in the monitor tree. To move a SiteScope in the monitor tree, the SiteScope must first be deleted from the monitor tree and then imported into another container.

A detached SiteScope can be attached again and Monitor Administration resumes control of the SiteScope. During the attach process, Mercury Business Availability Center synchronizes any data that may have changed while the SiteScope was detached.

It is recommended not to delete a SiteScope that has been detached from Monitor Administration. If a detached SiteScope is deleted from Monitor Administration, the SiteScope continues sending monitoring data to Mercury Business Availability Center, despite the fact that it no longer appears in Monitor Administration's monitor tree. To avoid this situation, it is recommended that a detached SiteScope be attached again before deleting.

To add a deleted SiteScope back to the monitor tree, you must go through the procedure for adding a SiteScope from the beginning.

To detach a SiteScope:

Select from the following options:

- In the monitor tree, right-click the SiteScope you want to detach and select **Detach** from the menu.
- In the Contents tab with the SiteScope highlighted, click the **Detach** button.

The SiteScope and all its child objects remain as uneditable objects in the monitor tree. You cannot add monitors, alerts, or reports, or configure settings or preferences for the SiteScope.

Note: You can perform the detach operation also from the SiteScope interface. This may be necessary if Monitor Administration is unavailable or if communication between Monitor Administration and the SiteScope has been interrupted. To detach, in the General Preferences page, click the **Detach** button.

You can access the SiteScope interface from the SiteScope installation or from within Monitor Administration by selecting the SiteScope tab.

To delete a SiteScope from the monitor tree:

Select from the following options:

- In the monitor tree, right-click the SiteScope you want to delete and select **Delete** from the menu.
- 
In the Contents tab with the SiteScope highlighted, click the **Delete** button.

The SiteScope is deleted from the monitor tree and no longer reports data to Mercury Business Availability Center.

Note: Deleting a SiteScope from the monitor tree does not delete that SiteScope's monitor configurations or disable monitoring on the SiteScope machine that was deleted.

To attach a previously detached SiteScope:

1 Select from the following options:

- In the monitor tree, right-click the SiteScope that has been detached and select **Attach** from the menu.
- In the Contents tab with the SiteScope highlighted, click the **Attach** button.

2 If any of the required fields are missing, the SiteScope properties page opens and you can enter the settings for port number, distributed settings, and any other settings that should be edited. For details on SiteScope settings, see "SiteScope Profile Integration Status" on page 6.

The SiteScope is now reattached and control of the SiteScope has been returned to Mercury Business Availability Center. During the attach process, Mercury Business Availability Center synchronizes any data that may have changed for the SiteScope while it was detached.

Part II

SiteScope Preferences

2

Introducing SiteScope Preferences

SiteScope allows you to set preferences and options for how SiteScope will integrate with your network environment. This includes defining profiles for connecting to other servers in the network, settings for connecting to e-mail, pager, and SNMP systems, schedule profiles, and user profiles.

This chapter describes:	On page:
Preferences Overview	25

Preferences Overview

Clicking the **Preferences** container on the monitor tree displays the Preferences content page. The Preference content page lists preference containers. Click on the name of an applicable Preference type name in the container list or on the monitor tree to display the contents of the applicable container.

The following table is a overview of the preference settings and definitions that can be configured using SiteScope Preferences. For more information about how to work with these settings, see the applicable preference setting page:

Preference Option	Description	Format
SiteScope General Preferences (for details see page 33)	Enter standard SiteScope license keys, license keys for optional monitor features, control SiteScope display options and features, and set SiteScope security options.	global settings
Windows Remote Preferences (for details see page 93)	Define and configure connectivity profiles for connecting to and monitoring remote Windows servers.	individual connection profiles
UNIX Remote Preferences (for details see page 81)	Define and configure connectivity profiles for connecting to and monitoring remote UNIX/Linux servers.	individual connection profiles
Logging Preferences (for details see page 43)	Select how long SiteScope should maintain monitor data locally or configure connectivity settings for exporting monitor data to an external database.	global log settings
E-mail Preferences (for details see page 51)	Define e-mail server settings and e-mail profiles for use with SiteScope E-mail Alerts.	global settings and optional e-mail recipient profiles
Pager Preferences (for details see page 59)	Define connection and command settings and pager profiles for using SiteScope Pager Alerts.	global settings and optional pager recipient profiles
SNMP Trap Preferences (for details see page 75)	Define settings and profiles SiteScope can use to send SNMP Trap Alerts.	global settings and optional SNMP trap profiles

Preference Option	Description	Format
Absolute Schedule Preferences (for details see page 29)	Define and manage custom schedules for running SiteScope monitors at specific times during the week.	individual schedules
Range Schedule Preferences (for details see page 69)	Define and manage custom schedules for running or disabling SiteScope monitors and alerts during a specific time period.	individual schedule ranges

3

Absolute Schedule Preferences

Around the clock operation has become a minimal standard for online commerce and networked services. SiteScope is designed for monitoring system availability 24/7. There may be situations where you want SiteScope run certain monitors only at specific times. SiteScope Absolute Schedules allow you to customize the operation of SiteScope monitors and alerts to fit special schedule requirements.

This chapter describes:	On page:
Working with Absolute Schedules	29
Adding a New Absolute Schedule	31

Working with Absolute Schedules

By default, SiteScope monitors, alerts, and reports are enabled 24 hours a day, 7 days a week, 365 days a year. This means that as long as a monitor is enabled, it will be 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 will attempt to run the monitor every 30 seconds throughout the day. If SiteScope detects an error condition, any associated alert will be executed as well, regardless of the time of day.

Normally, 24/7 monitoring is required for adequate monitoring of systems that are required to be available around the clock. However, there may be a number of situations where it is useful to enable certain SiteScope actions to correspond with a single event or a particular time of day. You use Absolute Schedules to instruct SiteScope to enable monitors according to an absolute time that you define.

Absolute Scheduling lets you set specific times that a monitor will be run on a weekly basis. Absolute schedules are reset at the end of the week and repeated each week.

Generally, Absolute Schedules will trigger a monitor to run **only once** at each time specified in the schedule. Absolute times are specified in a daily schedule. You may define multiple times for a monitor to run in a single day (for example, 6:00am, 12:00pm, and 6:00pm) by separating the times with a "," (comma). You may want to use this type of scheduling for monitors, such as the Link Checking monitor, which you want to only run once a day at a time when the server generally has a lighter load.

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

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 disabled for the period during which those monitors are disabled. However, if an alert is associated with other monitors that are not controlled by the same schedule, that alert will still be triggered if the other monitors report an error condition.

The times for Absolute Schedules are specified in the 24 hour format, also known as military format. This same syntax and format is used for both Range Schedules and Absolute Schedules. Examples of valid times entries are:

Schedule Entry	Description
10:23	10:23 AM, meaning 10:23 in the morning
23	11:00 PM
01,02:30,23:30	A multiple time entry including 1:00 AM, again at 2:30 AM, and again at 11:30 PM
00:00	12:00 AM or midnight

As shown by the third example, multiple times can be entered on a single day by separating the times by commas.

Note: Time values for range schedules must be limited to the 24 hour period of a standard day for each day. For example, you might want to disable monitors from 6:00 PM on Thursday evening until 8:00 AM the following morning. Entering a **from** value of 18 and a **to** value of 8 on the Thursday schedule will be invalid because the **to** value is actually referring to a time on Friday. To create such a schedule, you need to enter time values from 18 to 24 for Thursday and then enter from 0 to 8 for Friday.

Adding a New Absolute Schedule

Use the following steps to create a new Absolute Schedule.

To create a new Absolute Schedule:

1. Click on the **Preferences** container in the left menu tree. The content panel displays the **Preferences** container contents.
2. Click on the **Absolute Schedules** on the left menu tree or under the applicable section in the right Content panel. A list of current Absolute Schedule is displayed.
3. Click the **New Absolute Schedules** button near the top of the content panel. Alternately, you can right-click the container in the left menu to display the container action menu and select **New Absolute Schedules**. The New Absolute Schedule page is displayed.
4. Complete the items in the **Main Settings** section as described below. If necessary, complete the items in the **Advanced Settings** and other sections as described below.
5. When the required settings are defined, click the **Add** button to create the Absolute Schedule.

Absolute Schedule Settings

The following describes the settings used for Absolute Schedules.

Main Settings

You use the Main Settings section to enter information that defines the Absolute Schedule. Complete the Main Settings section for the Absolute Schedule as described below.

Name

Enter a text description for this Absolute Schedule definition. This name will be used to identify this Absolute Schedule definition in the product display.

Days of the Week

Enter the time or times that you want the monitor to run in the boxes next to the day of the week that you want the monitor to run. To enter multiple times for a single day, separate the times by a comma (,).

Advanced Settings

You use the Advanced Settings section to customize the Absolute Schedule. Complete the entries as needed and click the **Add** or **OK** button to save the settings.

Description

Enter an optional description text to further describe this Absolute Schedule. For example, you may enter some text describing the purpose or conditions relating to the use of this Absolute Schedule.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For details, see "Working with Categories" in *Working with Monitor Administration*.

4

SiteScope General Preferences

The General Preferences container is where you enter and view licensing information for SiteScope. You also use these settings to control other general display, optional features, and access options for SiteScope.

This chapter describes:	On page:
Configuring General Preferences Properties	33
Working in an I18N Environment	36
Using Default Authentication Credentials	38
Suspending Monitor Processes	39
Working with SiteScope Configuration Files	40

Configuring General Preferences Properties

Use the following steps to configure General Preferences properties.

To configure General Preferences properties:

1. Expand the SiteScope container element for which you want to configure the General Preferences properties and click on the **Preferences** container for that SiteScope. The content panel displays the **Preferences** container contents.
2. Click on the **General Preferences** link under the applicable container in the right hand panel. If necessary, click on the **Properties** tab in the upper right hand corner of the right hand panel to display the General Preferences Properties panel.

3 Click the **Edit** button at the bottom of the Properties panel. The Edit General Preferences page is displayed in the content panel.Alternately, you can right-click the **General Preferences** container in the left menu tree to display the container action menu and select **Edit Defaults**.

4 Complete the items in the **Main Settings** section as described below.

5 When the required settings are defined, click the **Ok** button to save the General Preferences settings.

Main Settings

You use the Main Settings section of the General Preferences Properties page to enable monitoring, options, and features controlled by the General Preferences settings. Complete the items for the General Preferences Properties as described below.

License Number

Enter your SiteScope license number to register your SiteScope monitors. This number is issued to you when you purchase a set of monitors. You must purchase a license if you intend to use SiteScope beyond the trial period.

License Status

This line displays information about the license as entered in the License Number box above. This includes the total number of monitor points permitted by the license and how many points have been used plus a label for any optional monitor license keys entered below.

Option Licenses

If you have purchased licensing for optional SiteScope monitoring capability, enter the license number in this text box. Normally, this license key will have a syntax similar to the SiteScope license entered above. If you have purchased multiple license keys, enter each key separated with a comma.

Locale-specific Date and Time

You select this option to have SiteScope display dates and times in a format that is applicable to a certain locale, country, or culture. The locale setting for the United States (US) is used by default. In order to use a different locale setting, you must modify the SiteScope configuration file to include the codes for the locale you want to use and select this option in the General Preferences Settings. Use the following steps to over-ride the default locale used by SiteScope:

To set a new locale to be used by SiteScope:

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

International Version

Check this option to enable international character sets. When this option is checked, SiteScope honors all character encodings. Use this option to instruct SiteScope to simultaneously handle character encodings from multiple sources and operating systems (for example, foreign language web pages). If not checked, only the default character set of the operation system where SiteScope installed is supported. The exceptions are all the URL monitor types, the Log File Monitor, and the File Monitor. These monitor types support multiple character encoding regardless of the International Version option setting.

Number of backups per file

Enter the number of SiteScope configuration file backups that you want to keep. This feature is to help preserve important monitor, alert, and general SiteScope configuration information (for example, the files in the <SiteScope install path>/SiteScope/groups directory). This number represents that number of backups per file that will be maintained. SiteScope will use a naming convention of filename.bak.1, filename.bak.2, ... filename.bak.#, where 1 is the latest backup file.

Working in an I18N Environment

SiteScope supports working in an I18N environment.

General Limitations

- Username, password, and URLs must be in English characters.
- Support for internationalization is available only in the new user interface.
- The host and the monitored machine must have the same locale. English is the default locale.
- The host can have a non-English locale in addition to English. For example, the monitored machine supports the German locale while the host supports German and English.

SiteScope Configuration

Perform the following steps to configure SiteScope for a non-English locale.

To configure SiteScope for a non-English locale:

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

Database Environment Issues

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

Monitors Tested for Internationalization

The following monitors have been tested for internationalization:

- CPU
- Database counter
- Database query
- Disk Space
- IIS Server
- Link Check
- Log File
- Memory
- Oracle 9i Application Server
- Ping
- Script
- Service
- SNMP
- SNMP trap
- SQL Server
- URL
- URL Content
- URL List
- URL Sequence

- Windows Event Log
- Windows Performance Counter
- Windows Resources

Using Default Authentication Credentials

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

1. no other authentication credentials are entered as part of an individual monitor configuration
2. the target application or system requires authentication credentials

The following monitor types can use this feature:

- URL Monitor
- URL Sequence Monitor
- Web Service Monitor

Complete the entries for default authentication as follows:

Default Authentication Username

Enter the default username to be used for authentication with remote systems. Both username and DOMAIN\username are valid formats. SiteScope will use this user name for the monitor types listed above unless a different user name is entered explicitly as part of the monitor configuration.

Default Authentication Password

Enter the default password to be used for authentication with remote systems. SiteScope will use this password for the monitor types listed above unless a different password is entered explicitly as part of the monitor configuration.

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 in order 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 using Monitor Administration. The **Suspend Monitors** option provides this function.

Suspend Monitors

Check this box to temporarily suspend the execution of all monitors. You can suspend all monitors temporarily, make configuration changes, and then resume monitoring again by clearing this option and save change.

Note: This option has the effect of disabling all monitors currently defined for this SiteScope installation. It is, however, not the same as a Disable all monitors action. If you set Suspend Monitors and then later clear this box to re-enable the monitors, those individual monitors that were set as disabled prior to the Suspend Monitors action will retain their original disabled state. This is different from a global disable action. If you were to select all monitors and Disable them (using the Manage Monitors and Groups page) and later re-enable them, the Disable state would be set and then cleared for all monitors, regardless of their state prior to the action.

Note: Using this option may impact reports. Monitors that would have run during the time that monitoring was suspended may display blanks for that period in reports.

Warning: There is currently no visual indication in the interface that a SiteScope is in a suspended monitor state. When the **Suspend Monitors** option is enabled, the following message is displayed in the corresponding SiteScope:

> SiteScope is in Suspended mode; no monitors are currently running.
> To reactivate monitoring, clear the Suspend Monitors setting on the General Preferences page.

Working with SiteScope Configuration Files

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

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

One possible advantage to disabling this option is that it may improve SiteScope performance.

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

Enable Configuration Files

This option enables the use of the master and monitor group configuration files for SiteScope version 8.x. When enabled, SiteScope will periodically check for changes to any files in the SiteScope\groups directory and update the binary configuration data accordingly.

5

Logging Preferences

Effective system availability monitoring requires that monitoring data be recorded and stored for an appropriate interval of time. Depending on the size of the data center, network, the number of servers and applications being monitored and the frequency of monitoring, managing the accumulated data can become challenging task in it self. You use SiteScope Logging Preferences options to control the accumulation and storage of monitor data.

This chapter describes:	On page:
Understanding SiteScope Logs and Data Logging Options	43
Setting SiteScope Log Preferences	44
Troubleshooting Database Connections	46
SiteScope Log Database Table Structure	48

Understanding SiteScope Logs and Data Logging Options

You use Logging Preferences to select how much monitor data will be accumulated and maintained on the SiteScope server or to configure 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. These data are stored as tab delimited text. SiteScope uses the log files to generate various management reports. Data records are needed for reporting on system availability and performance over time.

For monitor data results, a new, date-coded log file is created for each 24-hour period of monitoring. Eventually storage of the data logs can become a problem. You use Logging Preferences to select how many days of data log files SiteScope will maintain on the server before they are deleted. Alternately, you can limit the size of data logs.

SiteScope can also send monitoring data to an external database application. You can use this to reduce the data storage capacity of the SiteScope server and also make the monitoring data available to other reporting tools.

Setting SiteScope Log Preferences

Use the Logging Preferences properties to limit how much log information SiteScope saves to the local file system. The amount of data can be limited to the number of days to maintain log files or to a maximum data log file size.

Note: In order 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.

Enter the log preference options as indicated below and then click the **Save Changes** button located at the bottom of the form.

Main Settings

You use the Main Settings section of the Logging Preferences Properties page to enable monitoring, options, and features controlled by the Logging Preferences settings. Complete the items for the Logging Preferences Properties as described below.

Daily Logs To Keep

Enter the number of days of monitoring data to keep. Once a day, SiteScope deletes any logs older than the specified number of days. By default this is set to 40 days, which saves enough data to create monthly reports.

Note: Keeping monitor data logs for long periods can cause a data storage problem for the SiteScope server depending on the total number of monitors configured and how often the monitors run per day. You should monitor the size of the log files in the SiteScope\logs directory to estimate the data accumulation rate and adjust the **Daily Logs To Keep** setting or server resources as necessary.

Maximum Size of Logs

Enter the maximum size allowed for all monitoring logs. Once a day, SiteScope checks the total size of all monitoring logs and removes any old logs that are over the maximum size.

Note: By default, this setting is blank and not used as it can result in the loss of monitor report data.

Database Connection URL

To enable Database logging, enter a URL to a Database Connection. The easiest way to create a database connection is to use ODBC to create a named connection to a database. For example, first use the ODBC control panel to create a connection called SiteScopeLog. Then, enter jdbc:odbc:SiteScopeLog in this box as the connection URL.

Database Driver

Specify the database driver SiteSCope should use to connect to the database. The driver should be a JDBC driver. The default database driver is sun.jdbc.odbc.JdbcOdbcDriver. To have SiteScope use another driver the driver must also be installed in the **<SiteScope install path>/SiteScope/java** directory and the path and filename must be entered in this text box.

Database Username

Enter the username used to login to the database. If you are using Microsoft SQL server, you can leave this blank and choose NT Authentication when you setup the ODBC connection. With NT Authentication, SiteScope connects using the login account of the SiteScope service.

Database Password

Enter a password used to login to the database. If you are using Microsoft SQL server, you can leave this blank and choose NT Authentication when you create the ODBC connection. With NT Authentication, SiteScope connects using the login account of the SiteScope service.

Backup Database Connection URL

Optionally, you may enter a URL to a backup database. Use this option to provide failover of SiteScope database logging in the case that the primary database become unavailable.

Note: The same database table definition, database driver, user name and password are applied to both database connections.

After you save changes to the Database preferences, you need to stop and restart the SiteScope service to have the changes take effect.

Troubleshooting Database Connections

When Database logging is active and working correctly, you should see a table called SiteScopeLog in your database and a record added to the table every time a monitor runs. The data is sent to the database as a single table in a flat-file format. For additional details, see chapter on "SiteScope Log File Columns" in the SiteScope Reference Guide.

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

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

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

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

SiteScope Log Database Table Structure

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

Field Name	Example Data	Description
datex	1999-01-20 11:54:54	The first field contains the date that the monitor ran.
serverName	demo.sitescope.com	The second field contains the name of the server where SiteScope is running.
class	URLMonitor	The third field contains the type of the monitor
sample	23	The fourth field contains the sample number of this monitor
category	good	The fifth field contains the category name of the monitor
groupName	URLs	The sixth field contains the group name of the monitor
monitorName	Home Page	The seventh field contains the name of the monitor
status	1.01 seconds	The eighth field contains the status of the monitor

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) will correspond to the value listed as column 7 in the log files.

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

6

E-mail Preferences

Besides the visual icons and status messages displayed in the SiteScope interface, e-mail is the default media for sending event alerts when a problem has been detected by SiteScope. You use the E-mail Preferences to indicate the SMTP mail server, recipient addresses, and other settings that SiteScope should use when sending e-mail alerts and other SiteScope messages.

This chapter describes:	On page:
Working with SiteScope E-mail Preferences	51
Configuring E-mail Preferences Properties	52
Working with E-mail Recipient Profiles	54
E-mail Recipient Profile Settings	56

Working with SiteScope E-mail Preferences

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

You use the E-mail Preferences Properties panel to configure settings SiteScope needs in order to communicate with a external e-mail server. These are the default settings that SiteScope will use to send alerts as e-mail messages.

You use the Contents panel of the E-mail Preferences container to define custom E-Mail Recipient profiles to send e-mail alert messages to recipients other than the one defined in the Properties panel. The E-mail Recipient profile can then be associate with one or more E-mail alerts by editing the applicable alert definition.

Configuring E-mail Preferences Properties

Use the following steps to configure the default E-mail Preferences properties.

To configure E-mail Preferences properties:

1. Click on the **Preferences** container in the left menu tree. The **Preferences** container contents is displayed.
2. Click on the **E-Mail Preferences** link under the applicable container in the right hand panel. If necessary, click on the **Properties** tab in the upper right hand corner of the right hand panel to display the E-mail Preferences Properties panel.
3. Click the **Edit** button at the bottom of the Properties panel. The Edit E-mail Preferences page is displayed in the content panel.Alternately, you can right-click the **E-Mail Preferences** container in the left menu tree to display the container action menu and select **Edit Defaults**.
4. Complete the items in the **Main Settings** section as described below.
5. When the required settings are defined, click **OK** to save the E-mail Preferences settings.

Main Settings

You use the Main Settings section of the E-mail Preferences Properties page to specify E-mail infrastructure that will make up the default SiteScope E-mail Preferences settings. Complete the items for the E-mail Preferences Properties as described below.

Mail Server Domain Name

Enter the domain name of the SMTP mail server that SiteScope should use when sending e-mail messages. For example, mail.thiscompany.com. If you are unsure of your mail server's domain name, check with your Systems Administrator.

Administrator E-mail Address

Enter the e-mail address to which SiteScope should send status messages. For example, the administrator e-mail address might be sysadmin@thiscompany.com. SiteScope uses this address to send various status messages.

SiteScope Status Messages

Select which regular SiteScope status messages you want to receive. The options are:

- **Daily Status** - Select this option to have SiteScope send a brief daily status message to the administrator's e-mail address. This e-mail is scheduled to be generated at 7:07 AM every day. The subject of e-mail sent will include: "SiteScope daily status". The e-mail content includes the number of active monitors and groups, along with a URL link to the applicable SiteScope main page plus the version number of SiteScope installation.
- **SiteScope Starts/Restarts** - Select this option to have SiteScope send a brief message each time that SiteScope restarts. Normally, SiteScope will automatically restart itself once a day. Other restarts may be an indication of a monitor run problem. See the SiteScope Health page for more information.

From E-mail Address

Enter the e-mail address used as the From Address for mail generated by SiteScope. Specifying an e-mail address may make it easier for you to browse and sort e-mail sent by SiteScope. For example, you may want mail generated by SiteScope to come from sitescope@mycompany.com. If nothing is entered, the From E-mail Address will be the same as the address where the mail is sent.

Backup Mail Server Domain Name

Enter the domain name of the SMTP mail server that SiteScope should use whenever the primary mail server cannot be reached. For example, gateway.mycompany.com. If you are unsure of your backup mail server's domain name, check with your Systems Administrator.

Login

If access to the SMTP server you want SiteScope to use requires a login authentication, enter the username required by the SMTP server in this field. This username is used for both the primary and backup mail servers.

Password

If the SMTP server you want SiteScope to use requires authentication, enter the password for username entered in the **Login** field. This password is used for both the primary and backup mail servers.

Timeout

Enter an optional length of time (in seconds) to wait for a response from the SMTP server. The default value is 60 seconds. This is also the minimum value. If a response from the primary mail server is not received within the timeout period, SiteScope will switch to use the backup mail server.

Working with E-mail Recipient Profiles

The E-mail Recipients container page lists E-mail Recipient profiles that you use with SiteScope E-mail Alerts. This table lists the name of all the currently defined e-mail settings or profiles. You create and use the E-mail Recipient profiles for sending SiteScope e-mail alerts to individuals or groups other than the SiteScope Administrator e-mail entered on the E-mail Properties.

The following information is displayed in the content panel for each E-mail Recipient.

Name

This is the text name string assigned to the setting profile. You enter this name when you create a new e-mail recipient.

Description

This an optional text description string that can be assigned to the setting profile. You enter this description text in the Advanced Settings section when you create a new e-mail recipient.

You use the buttons in the Contents view to add, edit, or delete additional E-mail Recipient profiles.

Adding a New E-mail Recipient Profile

Use the following steps to create a new E-mail Recipient Profile.

To create a new E-mail Recipient Profile:

1. Click on the **Preferences** container in the left menu tree. The content panel displays the **Preferences** container contents.
2. Click on the **E-Mail Preferences** on the left menu tree or under the applicable section in the right Content panel. A list of current E-mail Recipient Profile is displayed.
3. Click the **New E-mail Preferences** button near the top of the content panel. Alternately, you can right-click the container in the left menu to display the container action menu and select **New E-mail Preferences**. The New E-mail Recipient Profile page is displayed.
4. Complete the items in the **Main Settings** section as described below. If necessary, complete the items in the **Advanced Settings** and other sections as described below.
5. When the required settings are defined, click the **Add** button to create the E-mail Recipient Profile.

Testing E-mail Recipient Profiles

Once you have created E-mail Recipient Profiles you can test them to confirm they are working and to troubleshoot problems. Use the following steps to test E-mail Recipient Profiles.

To test E-mail Recipient Profiles:

1. Click on the **Preferences** container in the left menu tree. The **Preferences** container contents is displayed.

2 Click the **E-Mail Preferences** container. The E-mail Preferences screen opens. If necessary, click the Contents tab to display the E-mail Recipient Profile container.

3 In the E-mail Recipient Profile table, check the box to the left of the E-mail Recipient Profile that you want to test.

4 Press the **Test** button on the menu bar at the bottom of the container. The Test Preferences dialogue screen opens. Details and possible errors in executing the action associated with the profile are displayed in the dialogue.

5 Click the **Close** button in the Test Preferences dialogue screen.

E-mail Recipient Profile Settings

The following describes the settings used for E-mail Recipient Profiles.

Main Settings

You use the Main Settings section to enter information that defines the E-mail Recipient Profile. Complete the Main Settings section for the E-mail Recipient Profile as described below.

Name

Enter a text description for this E-mail Recipient Profile definition. This name will be used to identify this E-mail Recipient Profile definition in the product display.

E-mail To

The e-mail address(es) that you want to send the alert to (for example, test@mycompany.com). You can enter multiple e-mail addresses by separating the e-mail addresses with commas (test@mycompany.com, sysadmin@thiscompany.com).

Disabled

Click this button to stop e-mail alerts from being sent to these e-mail addresses. You use this option to temporarily disable a particular e-mail without editing every alert that contains this e-mail setting

Advanced Settings

You use the Advanced Settings section to customize the E-mail Recipient Profile. Complete the entries as needed and click the **Add** or **OK** button to save the settings.

Description

Enter an optional description text to further describe this E-mail Recipient Profile. For example, you may enter some text describing the purpose or conditions relating to the use of this E-mail Recipient Profile.

Template

If you want e-mail alerts sent to these settings to use a particular template, then choose it from the drop-down list. Otherwise, whatever template is specified in the alert will be used. One you can use this feature is to define a single alert that will go to people and pagers, using the ShortMail template for the pagers.

Schedule

You use this option to specify when these e-mail settings should be enabled. By default, they are enabled every day of the week. You may select a more restricted schedule from the names schedules in the drop-down menu.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For details, see “Working with Categories” in *Working with Monitor Administration*.

7

Pager Preferences

Electronic pages are a useful way of sending an automated notification to system administrators who may not have immediate access to e-mail. Pager messages are also a method of alert escalation or to notify support personnel who may be away for the office. You use the Pager Preferences to configure settings and additional pager profiles that SiteScope will use for sending Pager alerts.

This chapter describes:	On page:
Working with SiteScope Pager Preferences	59
Configuring Pager Preferences Properties	60
Working with Pager Recipient Profiles	64
Pager Recipient Profile Settings	66

Working with SiteScope Pager Preferences

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

You use the Pager Preferences Properties panel to configure settings SiteScope needs in order to communicate with a external electronic paging service. These are the default settings that SiteScope will use to send alerts to an electronic pager.

You use the Contents panel of the Pager Preferences container to define custom Pager Recipient profiles to send pages to recipients other than the one defined in the Properties panel. The Pager Recipient profile can then be associate with one or more Pager alerts by editing the applicable alert definition.

Configuring Pager Preferences Properties

Use the following steps to configure the default Pager Preferences properties.

To configure Pager Preferences properties:

1. Click on the **Preferences** container in the left menu tree. The **Preferences** container contents is displayed.
2. Click on the **Pager Recipients** link under the applicable container in the right hand panel. If necessary, click on the **Properties** tab in the upper right hand corner of the right hand panel to display the Pager Preferences Properties panel.
3. Click the **Edit** button at the bottom of the Properties panel. The Edit Pager Preferences page is displayed in the content panel.Alternately, you can right-click the **Pager Recipients** container in the left menu tree to display the container action menu and select **Edit Defaults**.
4. Complete the items in the **Main Settings** section as described below.
5. When the required settings are defined, click **OK** to save the Pager Preferences settings.

Main Settings

You use the Main Settings section of the Pager Preferences Properties page to connect to a pager service provider Pager Preferences settings. Complete the items for the Pager Preferences Properties as described below.

Modem Port

Use the drop-down list to select the communications port that your modem is connected to on the SiteScope server. For SiteScope on Solaris or Linux, enter the path and device name for the modem. On the Windows NT/2000 platform, 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, you can 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 and right-click on the modem you want to use. Select Properties to view the properties for the modem. The properties should show the COM port number that is associated to the modem.

Connection Speed

Use the drop-down list to select the modem speed used for connections to your paging service. The default of 1200 baud is likely to work with most paging systems.

Pager Connection Options

There are four different methods for sending a message to your paging service.

- Modem-to-Modem Connection (Preferred)
- Dial and Enter Message
- Dial, Enter Command, and Enter Message
- Custom Modem Connection

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

Select the pager connection option you want SiteScope to use to send pages. Click the radio button to the left of the connection method you want to use and fill in the associated fields as indicated.

Modem-to-Modem Connection (Preferred)

Click the radio button to the left of this option if you have an alphanumeric pager and use an alphanumeric paging service. In the **Modem Number** text box, type the phone number to use for sending alphanumeric pages to the paging service modem. This number is provided by your paging service. Sometimes, the paging service will call this the TAP/IXO number. Some of the Modem Numbers for the larger services are:

- Airtouch: (800)326-0038
- MCI: (800) 555-0909
- Mobile Media: (800)622-5742
- Mobilecomm: (800)946-4644
- Pagenet: (800)720-8398
- PageMart: (800)864-9499
- SkyTel: (800)759-6366 or (800)679-2778
- USA Mobile: (800)589-9776

In the **PIN number** text box, type the last seven digits of the PIN number for your alphanumeric pager. Then Press the **Save Changes** button to save these settings.

Dial and Enter Message

Click the radio button to the left of this option if you dial a direct phone number to send a page. Most local paging companies work like this. In the **Phone number** text box, enter the phone number exactly as you would dial it from your telephone, including other numbers you might need such as a number to get an outside line. You can use dashes to make the number easier to read, but they are not required. 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.

For example, if you are dialing your pager from your office and you have to dial 9 to get an outside line, you might type:9, 555-6789.

Press the **Save Changes** button to save these settings.

Dial, Enter Command, and Enter Message

Click the radio button to the left of this option if you have a direct number, but need to enter a command before sending a page. Also, choose this option if your paging company uses a single phone number for all pagers and requests a PIN number before sending a page. In the **Phone number** text box, type the phone number exactly as you would dial it from your telephone, including other numbers you might need such as a number to get an outside line. You can use dashes to make the number easier to read, but they are not required. 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.

For example, if you are dialing your pager from your office where you have to dial 9 to get an outside line, you might type:9, 123-4567

In the **Send page command** text box, type the page command exactly as you would dial it from your touch tone telephone.

Press the **Save Changes** button to save these settings.

Custom Modem Connection

Click the radio button to the left of this option if your paging company does not use any of the previous connection choices. In the **Modem command** text box, type the entire modem command including the phone number to dial, any additional digits, and $message. SiteScope replaces $message with the message you specified for each alert. 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.

For 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.

Working with Pager Recipient Profiles

The Pager Recipients Contents view lists Pager Recipient profiles that you can use with SiteScope Pager Alerts. This view lists the name of all the currently defined Pager settings or profiles. You create and use different Pager Recipient profiles for sending SiteScope Pager alerts to individuals or groups other than the one defined in the Pager Recipient Properties.

The following information is displayed in the content panel for each Pager Recipient.

Name

This is the text name string assigned to the setting profile. You enter this name when you create a new pager recipient.

Description

This an optional text description string that can be assigned to the setting profile. You enter this description text in the Advanced Settings section when you create a new pager recipient.

You use the buttons in the Contents view to add, edit, or delete additional Pager Recipient profiles.

Adding a New Pager Recipient Profile

Use the following steps to create a new Pager Recipient Profile.

To create a new Pager Recipient Profile:

1 Click on the **Preferences** container in the left menu tree. The content panel displays the **Preferences** container contents.

2. Click on the **Pager Recipients** on the left menu tree or under the applicable section in the right Content panel. A list of current Pager Recipient Profile is displayed.
3. Click the **New Pager Preferences** button near the top of the content panel. Alternately, you can right-click the container in the left menu to display the container action menu and select **New Pager Preferences**. The New Pager Recipient Profile page is displayed.
4. Complete the items in the **Main Settings** section as described below. If necessary, complete the items in the **Advanced Settings** and other sections as described below.
5. When the required settings are defined, click the **Add** button to create the Pager Recipient Profile.

Testing Pager Recipient Profiles

Once you have created Pager Recipient Profiles you can test them to confirm they are working and to troubleshoot problems. Use the following steps to test Pager Recipient Profiles.

To test Pager Recipient Profiles:

1. Click on the **Preferences** container in the left menu tree. The **Preferences** container contents is displayed.
2. Click the **Pager Recipients** container. The Pager Preferences screen opens. If necessary, click the Contents tab to display the Pager Recipient Profile container.
3. In the Pager Recipient Profile table, check the box to the left of the Pager Recipient Profile that you want to test.
4. Press the **Test** button on the menu bar at the bottom of the container. The Test Preferences dialogue screen opens. Details and possible errors in executing the action associated with the profile are displayed in the dialogue.
5. Click the **Close** button in the Test Preferences dialogue screen.

Pager Recipient Profile Settings

The following describes the settings used for Pager Recipient Profiles.

Main Settings

You use the Main Settings section to enter information that defines the Pager Recipient Profile. Complete the Main Settings section for the Pager Recipient Profile as described below.

Name

Enter a text description for this Pager Recipient Profile definition. This name will be used to identify this Pager Recipient Profile definition in the product display.

Pager Connection Options

As with the default pager settings, there are four methods for sending a message to your paging service. Select the pager connection option you want SiteScope to use to send pages. Click the radio button to the left of the connection method you need to use and fill in the associated fields as indicated.

Modem-to-Modem Connection (Preferred)

Click the radio button to the left of this option if you have an alphanumeric pager and use an alphanumeric paging service. In the **Modem Number** text box, type the phone number to use for sending alphanumeric pages to the paging service modem.

In the **PIN number** text box, type the last seven digits of the PIN number for your alphanumeric pager.

Dial and Enter Message

Click the radio button to the left of this option if you dial a direct phone number to send a page. In the **Phone number** text box, enter the phone number exactly as you would dial it from your telephone, including other numbers you might need such as a number to get an outside line. Use commas to separate the portions of the phone number. Be sure to include any extra digits needed to get an outside line from your location.

Dial, Enter Command, and Enter Message

Click the radio button to the left of this option if you have a direct number, but need to enter a command before sending a page. Also, choose this option if your paging company uses a single phone number for all pagers and requests a PIN number before sending a page. In the **Phone number** text box, type the phone number exactly as you would dial it from your telephone, including other numbers you might need such as a number to get an outside line. Use commas to separate the portions of the phone number. Be sure to include any extra digits needed to get an outside line from your location.

In the **Send page command** text box, type the page command exactly as you would dial it from your touch tone telephone.

Custom Modem Connection

Click the radio button to the left of this option if your paging company does not use any of the previous connection option choices. In the **Modem command** text box, type the entire modem command including the phone number to dial, any additional digits, and $message. SiteScope replaces $message with the message you specified for each alert. Use commas to separate the portions of the phone number, command strings, and alert message strings.

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

Click this button to stop pages from being sent to this pager. You use this option to temporarily disable a particular pager without editing every alert that contains this persons pager. For example, when Joe goes on vacation you will want to disable his pager setting. Of course, you will also want to make sure that there is another pager specified for each alert that Joe is selected on so that someone will receive a page if there is a problem.

Advanced Settings

You use the Advanced Settings section to customize the Pager Recipient Profile. Complete the entries as needed and click the **Add** or **OK** button to save the settings.

Description

Enter an optional description text to further describe this Pager Recipient Profile. For example, you may enter some text describing the purpose or conditions relating to the use of this Pager Recipient Profile.

Schedule

You use this option to specify when these pager settings should be enabled. By default, they are enabled every day of the week. You may select a more restricted schedule from the names schedules in the drop-down menu.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For details, see "Working with Categories" in *Working with Monitor Administration*.

8

Range Schedule Preferences

Around the clock operation has become a minimal standard for online commerce and networked services. SiteScope is designed for monitoring system availability 24/7. There may be situations where you want SiteScope to change its monitoring and alerting behavior to match the schedules or certain operational groups or systems. SiteScope Range Schedules allow you to customize the operation of SiteScope monitors and alerts to fit special schedule requirements of your operation and organization.

This chapter describes:	On page:
Working with Range Schedules	69
Range Schedule Settings	72

Working with Range Schedules

By default, SiteScope monitors, alerts, and reports are enabled 24 hours a day, 7 days a week, 365 days a year. This means that as long as a monitor is enabled, it will be 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 will attempt to run the monitor every 30 seconds throughout the day. If SiteScope detects an error condition, any alert associated with the monitor will be executed as well, regardless of the time of day.

Normally, 24/7 monitoring is required for adequate monitoring of systems that are required to be available around the clock. However, there may be a number of situations where it is useful to enable and disable certain SiteScope actions based on the schedules of the individuals or groups responsible for the servers and systems being monitored. You use Range Schedules to instruct SiteScope to enable or disable monitors according to time periods that you define.

You can use Range Scheduling to specify a time range during which SiteScope will either enable or disable particular monitors. If you specify an enabled time range for a new monitor (using the Advanced Options on the Add monitor page), SiteScope will only run 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 will only be run during those times.

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

Range Schedules are inactive until they are explicitly associated with a monitor instance. You use the Advanced Settings section of a monitor configuration page to associate Range Schedules 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 disabled for the period during which those monitors are disabled. However, if an alert is associated with other monitors that are not controlled by the same schedule, that alert will still be triggered if the other monitors report an error condition.

Note: You can enter multiple ranges by entering several start times and several end time separated by commas. For example to disable from 2-3am and 7-8am, you would enter 2:00,3:00 to 7:00,8:00

SiteScope schedule times are specified in the 24 hour format, also known as military format. This same syntax and format is used for both Range Schedules and Absolute Schedules. Examples of valid times entries are:

Schedule Entry	Description
10:23	10:23 AM, meaning 10:23 in the morning
23	11:00 PM
01,02:30,23:30	A multiple time entry including 1:00 AM, again at 2:30 AM, and again at 11:30 PM)
00:00	12:00 AM or midnight

As shown by the third example, multiple times can be entered on a single day by separating the times by commas.

Adding a New Range Schedule

Use the following steps to create a new Range Schedule.

To create a new Range Schedule:

1. Click on the **Preferences** container in the left menu tree. The content panel displays the **Preferences** container contents.
2. Click on the **applicable preference object name** on the left menu tree or under the applicable section in the right Content panel. A list of current Range Schedule is displayed.
3. Click the **New Range Schedules** button near the top of the content panel. Alternately, you can right-click the container in the left menu to display the container action menu and select **New Range Schedules**. The New Range Schedule page is displayed.

4 Complete the items in the **Main Settings** section as described below. If necessary, complete the items in the **Advanced Settings** and other sections as described below.

5 When the required settings are defined, click the **Add** button to create the Range Schedule.

Range Schedule Settings

The following describes the settings used for Range Schedules.

Main Settings

You use the Main Settings section to enter information that defines the Range Schedule. Complete the Main Settings section for the Range Schedule as described below.

Name

Enter a text description for this Range Schedule definition. This name will be used to identify this Range Schedule definition in the product display.

Days of the Week

Enter the time or times that you want the monitor to run in the boxes next to the day of the week that you want the monitor to run. To enter multiple times for a single day, separate the times by a comma ",".

Range Schedules use a combination of a enable / disable setting and **from** and **to** time values to determine how SiteScope will schedule monitor runs. The following table presents several important examples for understanding, configuring, and using range schedules effectively.

Enable Setting (enable / disable)	Time Range (from / to)	Schedule Effect
enable	**from** and **to** time values specified	Monitors will be enabled to run only during time range between the **from** time and **to** time.
enable	(no time values specified)	Monitors will be enabled to run during all hours of the applicable day. This is the default setting for 24 hour operation.
disable	**from** and **to** time values specified	Monitors will be ENABLED to run during all hours of the applicable day EXCEPT during time range between the **from** time and **to** time. During the time range specified the monitors will be DISABLED.
disable	(no time values specified)	Monitors will be disabled during all hours of the applicable day. (It is important to note the difference between this disable method and the disable method where time values are specified.)

Note: Time values for range schedules must be limited to the 24 hour period of a standard day for each day. For example, you might want to disable monitors from 6:00 PM on Thursday evening until 8:00 AM the following morning. Entering a **from** value of 18 and a **to** value of 8 on the Thursday schedule will be invalid because the **to** value is actually referring to a time on Friday. To create such a schedule, you need to enter time values from 18 to 24 for Thursday and then enter from 0 to 8 for Friday.

Advanced Settings

You use the Advanced Settings section to customize the Range Schedule. Complete the entries as needed and click the **Add** or **OK** button to save the settings.

Description

Enter an optional description text to further describe this Range Schedule. For example, you may enter some text describing the purpose or conditions relating to the use of this Range Schedule.

Category Settings

The Category settings are used to filter items in the Monitor Administration views. For details, see "Working with Categories" in *Working with Monitor Administration*.

9

SNMP Trap Preferences

With the diversity of business systems and applications available, the interoperability of management applications can be important to overall system effectiveness and manageability. SiteScope can integrate with SNMP-based network management systems by using the SiteScope SNMP Trap Alert type. You use the SNMP Trap Preferences to define settings that are used by SiteScope SNMP Trap alerts when sending data to management consoles.

This chapter describes:	On page:
Working with SiteScope SNMP Trap Preferences	75
Configuring SNMP Trap Preferences Properties	76
Working with SNMP Trap Profiles	77
SNMP Trap Profile Settings	79

Working with SiteScope SNMP Trap Preferences

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

You use the SNMP Trap Preferences Properties panel to configure settings SiteScope needs in order to communicate with a external SNMP host or management console. These are the default SNMP parameters for use with SNMP Trap alerts.

You use the Contents panel of the SNMP Trap Preferences container to define custom SNMP Trap profiles to send traps to hosts other than the one defined in the Properties panel. The SNMP Trap profile can then be associate with one or more SNMP Trap alerts by editing the applicable alert definition.

Configuring SNMP Trap Preferences Properties

Use the following steps to configure the default SNMP Trap Preferences properties.

To configure SNMP Trap Preferences properties:

1. Click on the **Preferences** container in the left menu tree. The **Preferences** container contents is displayed.
2. Click on the **SNMP Trap Preferences** link under the applicable container in the right hand panel. If necessary, click on the **Properties** tab in the upper right hand corner of the right hand panel to display the SNMP Trap Preferences Properties panel.
3. Click the **Edit** button at the bottom of the Properties panel. The Edit SNMP Trap Preferences page is displayed in the content panel.Alternately, you can right-click the **SNMP Trap Preferences** container in the left menu tree to display the container action menu and select **Edit Defaults**.
4. Complete the items in the **Main Settings** section as described below.
5. When the required settings are defined, click **OK** to save the SNMP Trap Preferences settings.

Main Settings

You use the Main Settings section of the SNMP Trap Preferences Properties page to preference object action SNMP Trap Preferences settings. Complete the items for the SNMP Trap Preferences Properties as described below.

Send to Host

Enter the domain name or IP address of the machine that will receive all SNMP trap messages. This is machine must be running a SNMP console in order to receive the trap message. Examples of valid names are snmp.mydomain.com or 206.168.191.20.

SNMP Community

The default SNMP community name used for sending traps. The default community by most systems is public. The community string must match the community string used by the SNMP management console.

SNMP Trap Version

Select the default SNMP protocol version number to use. SNMP v1 and v2c are currently supported.

SNMP Trap ID

The type of trap to send. There are several predefined ID types for common conditions. You use the **Generic SNMP Trap ID** drop-down menu to select a generic SNMP type. To use an enterprise specific SNMP ID type, select the Other option in the **Generic SNMP Trap ID** drop-down menu and then enter the number of the specific trap type in the **Enterprise-Specific SNMP Trap ID** field.

SNMP Object ID

This identifies to the console the object that sent the message. There are several predefined objects to select from in the list. To use another OID, select Other... from this list and enter the other OID in the **Other SNMP Object ID** text box.

Other SNMP Object ID

Use this entry to specify an object ID other than those in the **SNMP Object ID** selection box. You must select Other... in the **SNMP Object ID** selection to enable this option.

Working with SNMP Trap Profiles

The SNMP Trap Preferences Contents view lists custom SNMP Trap profiles or templates that you create for use with SiteScope SNMP Alerts. This view lists the name of any additional SNMP Trap profiles. You create and use the SNMP Recipient profiles for sending SiteScope SNMP alerts to hosts or servers other than the SNMP host defined on the SNMPTrap Properties.

The following information is displayed in the content panel for each SNMP Recipient.

Name

This is the text name string assigned to the setting profile. You enter this name when you create a new SNMP recipient.

Description

This an optional text description string that can be assigned to the setting profile. You enter this description text in the Advanced Settings section when you create a new SNMP recipient.

You use the buttons in the Contents view to add, edit, or delete additional SNMP Trap profiles.

Adding a New SNMP Trap Profile

Use the following steps to create a new SNMP Trap Profile.

To create a new SNMP Trap Profile:

1. Click on the **Preferences** container in the left menu tree. The content panel displays the **Preferences** container contents.
2. Click on the **SNMP Trap Preferences** on the left menu tree or under the applicable section in the right Content panel. A list of current SNMP Trap Profile is displayed.
3. Click the **New SNMP Trap Preferences** button near the top of the content panel. Alternately, you can right-click the container in the left menu to display the container action menu and select **New SNMP Trap Preferences**. The New SNMP Trap Profile page is displayed.
4. Complete the items in the **Main Settings** section as described below. If necessary, complete the items in the **Advanced Settings** and other sections as described below.
5. When the required settings are defined, click the **Add** button to create the SNMP Trap Profile.

Testing SNMP Trap Profiles

Once you have created SNMP Trap Profiles you can test them to confirm they are working and to troubleshoot problems. Use the following steps to test SNMP Trap Profiles.

To test SNMP Trap Profiles:

1. Click on the **Preferences** container in the left menu tree. The **Preferences** container contents is displayed.

2. Click the **SNMP Trap Preferences** container. The SNMP Trap Preferences screen opens. If necessary, click the Contents tab to display the SNMP Trap Profile container.
3. In the SNMP Trap Profile table, check the box to the left of the SNMP Trap Profile that you want to test.
4. Press the **Test** button on the menu bar at the bottom of the container. The Test Preferences dialogue screen opens. Details and possible errors in executing the action associated with the profile are displayed in the dialogue.
5. Click the **Close** button in the Test Preferences dialogue screen.

SNMP Trap Profile Settings

The following describes the settings used for SNMP Trap Profiles.

Main Settings

You use the Main Settings section to enter information that defines the SNMP Trap Profile. Complete the Main Settings section for the SNMP Trap Profile as described below.

Name

Enter a text description for this SNMP Trap Profile definition. This name will be used to identify this SNMP Trap Profile definition in the product display.

Send to Host

Enter the host name of the machine to which this trap should be sent. For example, snmp.thiscompany.com. This machine must be running an SNMP console.

SNMP Community

Enter the SNMP community name used for this trap - usually this is "public".

SNMP Trap ID

The type of trap to send. There are several predefined ID types for common conditions. You use the **Generic SNMP Trap ID** drop-down menu to select a generic SNMP type. To use an enterprise specific SNMP ID type, select the "Other" option in the **Generic SNMP Trap ID** drop-down menu and then enter the number of the specific trap type in the **Enterprise-Specific SNMP Trap ID** field.

SNMP Trap Version

Select the SNMP protocol version number to use. SNMP v1 and v2c are currently supported.

SNMP Object ID

Indicate the SNMP object that is sending the trap. For example .1.3.6.1.2.1.1 is the "system" object from MIB-II (RFC 1213).

Advanced Settings

You use the Advanced Settings section to customize the SNMP Trap Profile. Complete the entries as needed and click the **Add** or **OK** button to save the settings.

Description

Enter an optional description text to further describe this SNMP Trap Profile. For example, you may enter some text describing the purpose or conditions relating to the use of this SNMP Trap Profile.

10

UNIX Remote Preferences

Today's business networks are often a mix of applications and services that are often run on different operating systems. Monitoring operation and performance across multiple platforms is both imperative and a challenge. 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.

This chapter describes:	On page:
Monitoring Remote UNIX Servers	81
Unix Server Profile Settings	83
Technical Notes on Remote UNIX Monitoring	89

Monitoring Remote UNIX Servers

SiteScope can monitor many applications independent of the platform they are run on by using Internet and other standard protocols such as SMTP, FTP, LDAP, and so forth. These types of systems and services can usually be monitored by sending requests using these platform-independent protocols. For example, checking that a Web server is responsive can be done using by making HTTP requests such as used by URL monitor types.

An important part of effective system monitoring involves monitoring resources at the server level. This is usually done by running commands specific to the operating system running on the server. This level of monitoring can be done using a login connection to the remote server.

SiteScope automates monitoring of server resources on remote UNIX servers by running command line tools on the remote machine as a remote user. To do this SiteScope must be able to establish a connection to the servers you want to monitor and be authenticated as a remote user having permissions to execute the applicable commands.

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

After you define a remote UNIX connection profile, you can create monitors to watch the resources of that server. Multiple monitors can use the same connection profile. Clicking the **Server** drop-down list on an Add Monitor page will display a list of the remote servers you have defined. You can then select the server that you want to monitor.

Adding a New Unix Server Profile

Use the following steps to create a new Unix Server Profile.

To create a new Unix Server Profile:

1. Expand the SiteScope container element for which you want to configure the Unix Server Profile and click on the **Preferences** container for that SiteScope. The content panel displays the **Preferences** container contents.
2. Click on the **Unix Remote Preferences** on the left menu tree or under the applicable section in the content panel. A list of current Unix Server Profile is displayed.
3. Click the **New UNIX Server** button near the top of the content panel. Alternately, you can right-click the container in the left Enterprise menu to display the container action menu and select **New UNIX Server**. The New Unix Server Profile page is displayed.
4. Complete the items in the **Main Settings** section as described below. If necessary, complete the items in the **Advanced Settings** and other sections as described below.

5 When the required settings are defined, click the **Add** button to create the Unix Server Profile.

Unix Server Profile Settings

The following describes the settings used for Unix Server Profiles.

Main Settings

You use the Main Settings section to enter information that defines the Unix Server Profile. Complete the Main Settings section for the Unix Server Profile as described below.

Host

The IP address or host name of the server you wish to monitor. If you are using the HTTP method of monitoring, enter the full URL of the CGI script (for example: http://demo.thiscompany.com/cgi-bin/run.sh) To use the same login credentials to configure multiple servers at the same time, enter the server addresses separated by commas. For example, if you are using NetBIOS to connect to other servers, you can enter a comma-separated string of server addresses such as: serveraddress1,serveraddress2,serveraddress3,serveraddress4. When you complete the other required entries on the form and click **OK**, SiteScope creates a new remote connection profile for each server address in the list.

Note: When adding multiple servers in a single operation, SiteScope does not automatically test connectivity with each server. You can click **Test** in the table listing the Unix Servers to test connectivity after the profiles have been added.

Login

The login for the remote server.

Password

The password for the remote server or the passphrase for the SSH key file. When using SSH authentication with public/private key based authentication enter the passphrase for the identity file here.

Name

A name by which the remote machine should be known in SiteScope. This name will appear in the drop-down list of the Choose Server page for monitors that can connect to remote servers.

Trace

Check this option to trace messages to and from the remote server in the RunMonitor.log file

OS

The operating system running on the remote server. This is required so that the correct information can be obtained from that server. Use the drop-down list feature to select from the default operating systems. SiteScope currently includes default support for the following versions of UNIX:

AIX	Linux	SGI Irix
FreeBSD	MacOSX	Sun Solaris
HP/UX	OPENSERVER	Tru64 5.x
HP/UX 64-bit	SCO	Tru64 Pre 4.x (Digital)

For servers running versions of UNIX which are not included in the list, see the section on Remote UNIX Adapter Kit in the Advanced SiteScope Topics section.

Method

The method for connecting to the server. The currently supported methods are:

Connection Method	Description
Telnet	Log in to the remote server using Telnet
SSH	Log in to the remote server using the SSH protocol. This may require additional software and setup depending on the version of UNIX you are working with. See the document on Secure Shell in the Advanced SiteScope Topics section for more information on SSH requirements.
Rlogin	Log in to the remote server using the Rlogin protocol
HTTP	Connect to an HTTP server on the remote server and run the command via a CGI. For this method the Login and Password are optional and are used for authorizing SiteScope to log on to the remote machine if required.

Prompt

This is the prompt output when the remote system is ready to handle a command - the default is #

Login Prompt

This is the prompt output when the system is waiting for the login to be entered - the default is "ogin:"

Password Prompt

This is the prompt output when the system is waiting for the password to be entered - the default is "assword:"

Secondary Prompt

In the case the telnet connection to the remote server causes the remote server to prompt for more information about the connection, enter the secondary prompt(s) here. Separate multiple prompt string by commas (,). For 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 you might need to enter Terminal type? as the secondary prompt. The response to the secondary prompt is entered in the **Secondary Response** box below.

Secondary Response

Enter the response(s) to any secondary prompts required to establish connections with this remote server. Separate multiple responses with commas (,).

Initialize Shell Environment

Enter any shell commands to be executed at beginning of the session. Separate multiple commands with a semicolon (;). You use this option to specify shell commands to be executed on the remote machine directly after a Telnet or SSH session has been initiated. These commands can be used to customize the shell for each SiteScope remote. Some example cases include:

- The remote shell may not have the correct path set for SiteScope scripts to run. The following command will add 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 will not be executed.

- There have been cases where the remote Telnet Server does not echo back the command line properly. This may cause strange behavior for monitors that rely on this behavior. Enter the following command to force the remote terminal to echo: `stty echo`

➤ Certain UNIX shells have been known to behave erratically with SiteScope. This includes bash, ksh, and csh. Enter the following command to change the shell to sh for the SiteScope connection: /bin/sh

Remote Machine Encoding

If the remote server is running an operating system version that uses a different character encoding than the server on which SiteScope is running, enter the encoding to use for the remote server. This will enable SiteScope to display encoded content correctly. By default, SiteScope uses Cp1252 encoding. Examples of other encodings are Cp1251, Cp1256, Shift_JIS and EUC_JP.

Advanced Settings

You use the Advanced Settings section to customize the Unix Server Profile. Complete the entries as needed and click the **Add** or **OK** button to save the settings.

Description

Enter an optional description text to further describe this Unix Server Profile. For example, you may enter some text describing the purpose or conditions relating to the use of this Unix Server Profile.

SSH Connection Method

The client to use for this connection. The currently supported clients are:

Client	Description
Internal Java Libraries	Connect using the Java SSH client integrated with SiteScope.
Plink/External SSH Client	Connect using an external SSH client. On NT, SiteScope ships with Plink on UNIX or Linux SiteScope will use an installed client such as OpenSSH.

SSH Port Number

Enter the port that the remote SSH server is listening on.

Disable Connection Caching

Check this option to turn off connection caching for this remote. By default SiteScope caches open connections.

Connection Limit

This setting controls the number of open connections that SiteScope will allow for this remote. If you have a large number of monitors configured to use this connection then set this number high enough to relieve the potential bottleneck.

Note: This setting does not effect the running of tests for a remote, tests will always create a new connection.

SSH Authentication Method

The authentication method to use for SSH connections. The currently supported methods are:

Authentication	Description
Password	Authenticate using a password.
Key File	Authenticate using public/private key authentication. When this option is selected SiteScope uses the private key in the file **SiteScope/groups/identity** to authenticate. The corresponding public key must be listed in the authorized_keys file on the remote host. See the document on Secure Shell in the Advanced SiteScope Topics section for more information on SSH requirements.

Key File for SSH connections

Select the file that contains the private key for this connection. The default key file is **SiteScope\groups\identity**. This setting only applies when the authentication method is Key File .

SSH Version 2 Only

Check this option to force SiteScope to use SSH protocol version 2 only. This option only applies when using the integrated Java Client. See the section on Configuring SSH Using an External Client for information on configuring an external SSH client to use SSH2 protocol.

Custom Commandline

Enter a custom commandline for a remote using the External Client. This option can be used when needing to pass specific options to the external client being executed. Valid substitution variable are

- $root$: This will be translated to the SiteScope directory.
- $user$: This will be translated to the username entered into the remote.
- $password$: This will be translated to the password entered into the remote.
- $host$: This will be translated to the hostname entered into the remote.

Use the following steps to add a remote UNIX server profile to SiteScope.

Technical Notes on Remote UNIX Monitoring

The following is additional information relating to the setup of remote UNIX servers in SiteScope and the monitoring of remote UNIX server performance.

Connection Methods for Remote UNIX

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

telnet

Along with SSH, telnet is another popular method for connecting to remote UNIX servers. You can set up your remote servers to require a password for telnet, or to allow access without a password (like "rsh"). SiteScope will handle either case.

SSH

For Solaris, using the SSH access method requires that an SSH client is installed on the SiteScope machine and the SSH server installed on the servers you are monitoring. See the document on Secure Shell in the Advanced SiteScope Topics section for more information on SSH requirements. The path to the SSH client on the machine where SiteScope is running should be:
/usr/local/bin/ssh or /usr/bin/ssh

For Windows NT or 2000, an SSH client is included in the package. For debugging, the Windows SSH client can be run from the command line, replacing the values for the username, host name, and password:\SiteScope\tools\plink.exe -ssh myUser@myServer.myCompany.com -pw myPassword

Using SSH requires that digital certificates be installed on each of the servers you will be connecting to.

rlogin

You can set up your remote servers to require a password for rlogin, or to allow access without a password (like "rsh"). SiteScope will handle either case.

HTTP

There are some cases where it may be useful to use a Common Gateway Interface program over HTTP to access performance data or application data from a UNIX server. Two simple CGI scripts are included with SiteScope to allow access over HTTP: **<SiteScope root directory>/WEB-INF/classes/CustomRemote/examples/remote.pl** and **<SiteScope root directory>/WEB-INF/classes/CustomRemote/examples/remote.sh**

The remote.pl CGI is a Perl (version 4 and above) script that executes a command on the server; the remote.sh script does the same, except as a UNIX sh script. CGI commands are passed in via the COMMAND CGI variable. If you are using the CGI connection method and you want to use remote actions, remember that the permissions for both the directory containing the CGI script and the /script directory need to allow the Web server (probably running as a user with few permissions) to execute in those directories. Additionally, the scripts need to have execute permission.

If you wish to use a CGI script that puts more restrictive limits on the commands that can be run, you can use a different CGI script. All that matters is that the CGI returns the output of the command passed in via the COMMAND variable. For greater security, you can set up your Web server to require a login/password authorization to run the script (this is recommended). Also, if you have a secure Web Server on that server, you can set up the script to run using the Secure Sockets Layer (SSL, used in https requests), so that the request and output is encrypted.

We are open to requests for additional connection modes and the API for writing connectors is available. We have also included information on how to create an adapter file to remotely monitor versions of UNIX that are not currently supported as one of the SiteScope defaults. In either case, contact SiteScope support at http://support.mercuryinteractive.com/ and we can discuss adding a connector that fits your specific needs. A sample connector Java class, which outlines the structure of a connector, can be found in the following directory: **<SiteScope install path>/SiteScope/classes/CustomRemote/examples**

If you choose to write one yourself, let us know - we'd like to hear about your experience.

11

Windows Remote Preferences

Today's business networks are often a mix of applications and services that may be run on more than one operating systems. Monitoring operation and performance across multiple platforms is both imperative and a challenge. 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 resource such as CPU, Disk Space, Memory, and services as well as Windows specific Performance Counter data.

This chapter describes:	On page:
Monitoring Remote Windows Servers	93
Windows Server Profile Settings	96
Technical Notes on Remote Windows Monitoring	100

Monitoring Remote Windows Servers

SiteScope can monitor many applications independent of the platform they are run on by using Internet and other standard protocols such as SMTP, FTP, LDAP, and so forth,. These types of systems and services can usually be monitored by sending requests using these platform-independent protocols. For example, checking that a Web server is responsive can be done using by making HTTP requests such as used by URL monitor types.

An important part of effective system monitoring involves monitoring resources at the server level. This is usually done by running commands specific to the operating system running on the server. This level of monitoring can be done using a login connection to the remote server.

SiteScope automates monitoring of server resources on remote Windows servers by running tools that access data on the remote machine. To do this SiteScope must be able to establish a connection to the servers you want to monitor and be authenticated as a user having permissions to permission to access the NT performance registry on the remote machine.

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

- Define an individual Remote Windows Server connection profile for each server
- Permit SiteScope to access remote servers by setting domain privileges

These two methods are described in the following sections.

Remote Windows Server Connection Profiles

Monitoring of 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 login to a remote server and to access the Windows performance registry on that remote machine. To be able to use this method you will also need to 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. This applies for monitoring servers running Windows operating systems from SiteScope running on Windows and when using an SSH connection from SiteScope running on UNIX.

Setting Domain Privileges for SiteScope Monitoring

SiteScope for Windows will automatically populate a list of servers that are visible in the local domain for selection for the Choose Server page for monitor types that require that a server 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. There are three options that can be used to enable monitoring in this environment:

1 **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 will give SiteScope access to monitor server data within the domain.

2 **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.

3 **Edit the registry access permissions for all machines in the domain to allow non-admin access.** See the Microsoft Knowledge Base Article - 158438 for details on Enabling Non-Admin Users to Remotely Monitor with PERFMON. 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 will include all machine in the domain, only those where the registry has been modified can be monitored without use of a connection profile.

After you provide the necessary domain administration privileges or define a Windows Server connection profile, you can create monitors to watch the resources and performance counters for that server. Multiple monitors can use the same connection profile.

Adding a New Windows Server Profile

Use the following steps to create a new Windows Server Profile.

To create a new Windows Server Profile:

1 Expand the SiteScope container element for which you want to configure the Windows Server Profile and click on the **Preferences** container for that SiteScope. The content panel displays the **Preferences** container contents.

2 Click on the **Windows Remote Preferences** on the left menu tree or under the applicable section in the content panel. A list of current Windows Server Profile is displayed.

3 Click the **New Windows Remote Preferences** button near the top of the content panel. Alternately, you can right-click the container in the left Enterprise menu to display the container action menu and select **New Windows Remote Preferences**. The New Windows Server Profile page is displayed.

4 Complete the items in the **Main Settings** section as described below. If necessary, complete the items in the **Advanced Settings** and other sections as described below.

5 When the required settings are defined, click the **Add** button to create the Windows Server Profile.

After defining the Windows Remote Preferences definition for SiteScope, you can have SiteScope test the settings by clicking on the **Test** link for the applicable server in the Remote NT Server table.

Windows Server Profile Settings

The following describes the settings used for Windows Server Profiles.

Main Settings

You use the Main Settings section to enter information that defines the Windows Server Profile. Complete the Main Settings section for the Windows Server Profile as described below.

Host

The IP address or UNC style name of the NT server you wish to monitor. An IP hostname will also work provided that the SiteScope server has a way to resolve this common name into an IP address (for example, by the use of a hosts file, DNS, or WINS/DNS integration). To use the same login credentials to configure multiple servers at the same time, enter the server addresses separated by commas. For example, if you are using NetBIOS to connect to other servers in an NT domain, you can enter a comma-separated string of server addresses such as: \\server1,\\server2,\\server3,\\server4. When you complete the other required entries on the form and click **Add** Remote NT Server, SiteScope creates a new remote connection profile for each server address in the list.

Note: When adding multiple servers in a single operation, SiteScope does not automatically test connectivity with each server. You can use the **Test** links in the Remote NT Server Table to test connectivity after the profiles have been added.

Login

The login for the remote server. If the server is within the same domain as the SiteScope machine, include the domain name in front of the user login name. For example: <domainname>\<user>. If you are 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>\<user>.

Password

The password for the remote server or the passphrase for the SSH key file. When using SSH authentication with public/private key based authentication enter the passphrase for the identity file here.

Name

A name by which the remote machine should be known. This name will appear in the **Server** drop-down list of monitors that can use this connection profile.

Trace

Check this box to have trace messages to and from the subject server recorded to the SiteScope RunMonitor.log file.

Method

SiteScope can use one of two connection types for monitoring Windows server resources. These are:

- NetBIOS - the default server-to-server communication protocol for Windows NT and 2000 networks.

➤ SSH - Secure Shell, a more secure communication protocol that can be installed on Windows NT/2000 based networks. This connection method normally requires installing SSH libraries on each server to which you want to connect. See the document on Secure Shell in the Advanced SiteScope Topics section for more information

Remote Machine Encoding

If the remote server is running an operating system version that uses a different character encoding than the server on which SiteScope is running, enter the encoding to use for the remote server. This will enable SiteScope to display encoded content correctly. By default, SiteScope uses Cp1252 encoding. Examples of other encodings are Cp1251, Cp1256, Shift_JIS and EUC_JP.

Advanced Settings

You use the Advanced Settings section to customize the Windows Server Profile. Complete the entries as needed and click the **Add** or **OK** button to save the settings.

Description

Enter an optional description text to further describe this Windows Server Profile. For example, you may enter some text describing the purpose or conditions relating to the use of this Windows Server Profile.

SSH Connection Method

The SSH client to use for this connection. The currently supported clients are:

Client	Description
Internal Java Libraries	Connect using the Java SSH client integrated with SiteScope.
Plink/External SSH Client	Connect using an external SSH client. On NT, SiteScope ships with Plink on UNIX or Linux SiteScope will use an installed client such as OpenSSH.

SSH Port Number

Enter the port that the remote SSH server is listening on.

Disable Connection Caching

Check this option to turn off connection caching for this remote. By default SiteScope caches open connections.

Connection Limit

This setting controls the number of open connections that SiteScope will allow for this remote. If you have a large number of monitors configured to use this connection then set this number high enough to relieve the potential bottleneck.

Note: This setting does not effect the running of tests for a remote, tests will always create a new connection.

SSH Authentication Method

The authentication method to use for SSH connections. The currently supported methods are:

Authentication	Description
Password	Authenticate using a password.
Key File	Authenticate using public/private key authentication. When this option is selected SiteScope uses the private key in the file **SiteScope/groups/identity** to authenticate. The corresponding public key must be listed in the authorized_keys file on the remote host. See the document on Secure Shell in the Advanced SiteScope Topics section for more information on SSH requirements.

Key File for SSH connections

Select the file that contains the private key for this connection. The default key file is SiteScope\groups\identity. This setting only applies when the authentication method is Key File .

SSH Version 2

Check this option to force SiteScope to use SSH protocol version 2 only. This option only applies when using the integrated Java Client in SiteScope. See the section on Configuring SSH Using an External Client for information on configuring an external SSH client to use SSH2 protocol.

Custom Commandline

Enter a custom commandline for a remote using the External Client. This option can be used when needing to pass specific options to the external client being executed. Valid substitution variable are

- $root$: This will be translated to the SiteScope directory.
- $user$: This will be translated to the username entered into the remote.
- $password$: This will be translated to the password entered into the remote.
- $host$: This will be translated to the hostname entered into the remote.

Technical Notes on Remote Windows Monitoring

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

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

For security reasons, SiteScope may not be allowed to use the permissions of a full administrator account. SiteScope can be granted restricted monitoring access by editing certain Windows Registry Keys. See the Enabling Non-Admin Users to Remotely Monitor with PERFMON support note on the Microsoft support site for more information.

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

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

Troubleshooting Windows Event Log Access on Remote Windows Servers

Problem
When viewing Remote Windows event logs or getting alerts relating to monitoring a remote Windows machine, you see:
The description for Event ID (XXXX) in Source (XXXX) could not be found. It contains the following insertion string(s):
The operation has completed successfully.

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

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

1 Locate on the remote machine which event you are not getting properly in SiteScope by finding the entry in the Event Viewer. Write down the information for the event id, source 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 (that is, MSExchangeSA)

3 Click the EventMessageFile and write down the data for where that DLL is located. (that is, C:\EXCHSRVR\bin\madmsg.dll)

4 Now, you need to locate the DLL on the remote and copy it to the SiteScope machine. You can copy this one of two ways:

- The Initlog.exe utility, in the "BackOffice Resource Kit, Second Edition," can be used 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), OR
- Using ftp, mail, etc 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. So, you must create the same folder structure as in step 3 and place the file in that directory. Otherwise, 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 DLL on BOTH machines. Also, if you do this, you will need to update the registry in step 3 to reflect the directory the DLL is in.

Using Perfex for Troubleshooting Remote Windows Connections

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

1 Open a command window on the SiteScope server.

2 Change directory to the **<SiteScope install path>\SiteScope\tools** directory.

3 Type in the following command line:
perfex \\MACHINE -u username -p password -d -elast "Application"

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

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

4 Usually, you will want to list only the last 10 or 12 events in order 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
```

This will produce a lot of output so go through each entry until you find the one you need.

5 Once you find the record you are looking for, note the Record id for easier searching next time when using the command in Step 3.

6 This output will tell you what data SiteScope is receiving. For 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,you will see 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.

Part III

SiteScope Health

12

Monitoring SiteScope Server Health

For reliability of operations monitoring depends in part on the reliability of the monitoring application. SiteScope can monitor several key aspects of its own environment to help uncover monitor configuration problems as well as SiteScope server load. Optionally, SiteScope can also monitor its connectivity and related data events when connected to Mercury Business Availability Center.

This chapter describes:	On page:
About the SiteScope Health Group	107
Adding SiteScope Health Monitors	108
Understanding SiteScope Health Monitoring	109

About the SiteScope Health Group

Beginning in SiteScope version 7.9.1.0, SiteScope Health is a specially designed group of monitors that display information about SiteScope's own health. This includes monitoring server resource usage, key processes, monitor load, and the integrity of key configuration files used by SiteScope. SiteScope Health monitoring data is also recorded in the daily monitor logs, by default, so you can create reports on SiteScope Health performance.

The Health monitor group is displayed as a special health icon within the main SiteScope container. You view the contents of the Health monitor group by clicking the **Health** container.

SiteScope Health monitoring includes six special monitor types. A description of these monitors is shown in the following table:

Monitor Type	Default Name	Description
Log Event Health Monitor	Log Event Checker	Checks for certain events logged to the SiteScope error log
Monitor Load Monitor	Monitor Load Checker	Checks for data about the number of monitors being run or waiting to run
Health of SiteScope Server Monitor	Health of SiteScope Server	Checks a large number of server process and resources for the server on which SiteScope is running

See the SiteScope Health Monitor Reference section for more information about the configuration of the individual SiteScope Health Monitors.

As with other SiteScope monitors and groups, you may associate alerts and reports with individual Health monitors to be notified of problems and review SiteScope performance over time.

Adding SiteScope Health Monitors

SiteScope Health monitors are enabled automatically when SiteScope is deployed. This means that the monitors will normally be present when you import a SiteScope to Monitor Administration. If it is necessary to add SiteScope Health monitors to a SiteScope installation, you use a Health Template available in the monitor tree. The special monitor templates are deployed into the Health monitor group of the SiteScope you want to monitor. You use the following steps to deploy a set of SiteScope Health monitors.

To deploy SiteScope Health Monitors:

1 Open the SiteScope container to which you want to display the Health Monitors. Confirm that the SiteScope includes the Health monitor group container.

Note: The Health monitor group container is identified with a special health indicator icon

---

2. Find the **Health Templates** in the monitor tree. Click to expand the container contents. The available Health monitor templates are displayed.
3. Select the Health monitor template for the operating system on which the SiteScope you want to monitor is running. The choices are:

   UNIX Health Monitors

   Windows Health Monitors
4. Right-click on the template icon and select **Copy** from the action menu.
5. Right-click on the **Health** monitor group container of the SiteScope to which you want to deploy the Health monitors and select **Paste** from the Action menu. The monitors in the selected template are then configured and deployed to the selected SiteScope server.

Understanding SiteScope Health Monitoring

This section contains information about how to interpret the results of SiteScope Health Monitoring and some actions to take if errors are detected. See "SiteScope Health Monitor Reference" for more details on the specific SiteScope Health monitor measurements.

SiteScope Log Events

The Log Event Monitor is the equivalent of a SiteScope monitor group that watches the SiteScope Error Log (`error.log`) for certain events. These events include Log entries indicating that a monitor has been "skipped" or there was a problem in reporting data to another application.

A SiteScope monitor will be reported as "skipped" if the monitor fails to complete its actions before it is scheduled to run again. This can occur with monitors that have complex actions to perform, such as querying databases, stepping through multi-page URL sequences, waiting for scripts to run, or waiting for an application that has hung. This can also happen if there are too many monitors waiting to run that require a process from the process pool.

For example, assume you have a URL Sequence Monitor that is configured to transit a series of eight Web pages. This sequence includes performing a search which may have a slow response time. The monitor is set to run once every 60 seconds. When the system is responding well, the monitor can run to completion in 45 seconds. However, at times, the search request takes longer and then it takes up to 90 seconds to complete the transaction. In this case, the monitor will not have completed before SiteScope is scheduled to run the monitor again. SiteScope will detect this and make a log event in the SiteScope error log. The SiteScope Log Event Monitor will detect this signal an error status.

A monitor may also skip if it is a monitor type that requires a process from the process pool but the process pool limit has been reached. Generally, this is not likely to happen but may occur in some situations with high monitoring load. The SiteScope Health Log Event Monitor also watches for process pool events.

Skipped monitors cause a number of problems. One is the loss of data when a monitor run is suspended due because a previous run has not completed or has become hung by a unresponsive application. Skipped monitors can also cause SiteScope to automatically stop and restart itself, an event that is also monitored by the SiteScope Health Log Event Monitor. A restart is done in an effort to clear problems and reset monitors. However, this can also lead to gaps in monitoring coverage and data. Adjusting the run frequency (**Frequency**) at which a monitor is set to run or specifying an applicable timeout value can often correct the problem of skipping monitors. Investigation of unresponsive systems that are being monitored may also be necessary.

Note: A Max Monitor Skipping setting has been added to allow monitors that are skipping to be disabled automatically. If this occurs, SiteScope is not restarted but an e-mail is sent to the SiteScope administrator about the skipping monitor to signal the disable event. This optional functionality is disabled by default but can be enabled by changing the `_shutdownOnSkips` to remove the value in the `master.config` file or remove the setting entirely.

Note: A setting for controlling the maximum number of processes available is available in the `master.config` file. The default is `_processPoolMaxPerPool=50`. You should only change this setting if adjustments to monitor configurations do not resolve the monitor performance problems.

The Log Event Monitor is also configured to report log events that indicate a problem with the transfer of SiteScope monitor and configuration data to a Mercury Business Availability Center installation. See the section on Integration with Mercury Business Availability Center for more information on Troubleshooting Data Reporting to Business Availability Center.

SiteScope Monitor Load

The Monitor Load Monitor is the equivalent of a SiteScope monitor group that watches how many monitors are running and how many are waiting to be run. Watching monitor load is important to help maintain monitoring performance and continuity. If the number monitors waiting approaches or exceeds the number of monitors running, adjustments should be made to monitor configurations to reduce the number of monitors waiting to run. Generally, this can be done by reducing the run frequency of some monitors.

SiteScope Server Health

The Health of SiteScope Server Monitor is the equivalent of a SiteScope monitor group that monitors server resources on the server where SiteScope is running. This includes monitors for CPU, disk space, memory, and key processes. A problem with resource usage on the SiteScope server may be caused by monitors with configuration problems or may simply indicate that a particular SiteScope is reaching it performance capacity. For example, high CPU usage by SiteScope may indicate that the total number of monitors being run is reaching a limit. High disk space usage may indicate that the SiteScope monitor data logs are about to exceed the capacity of the local disk drives (see the section on Log Preferences for SiteScope data logging options).

13

SiteScope Health Monitor Reference

SiteScope Health Monitors are deployed by using the Health group page. The error, warning, and good status thresholds for these monitors are set in the same way as for other monitor types.

This chapter describes:	On page:
Log Event Health Monitor	113
Monitor Load Monitor	115
Health of SiteScope Server Monitor	116

Log Event Health Monitor

This monitor is designed to check the `error.log` file for the local SiteScope installation. You can edit the counters, the update frequency and the display name for this monitor type. Click **Get Counters** to edit the counters selected for the monitor. You can use the Advanced Settings to disable the monitor individually as well as selecting other options as shown on the monitor properties panel.

The status thresholds for this monitor are based on the counters selected. The counters for this monitor type are listed in the table below.

Note: Only the first 15 selected counters will be configured and monitored. A maximum of 10 measurements can be used as status threshold criteria for alerting.

Log Event Monitor Counters

The following tables lists all the available counters for this health monitor.

Counter	Description
skipped #1	A monitor has skipped its scheduled run once
skipped #2	A monitor has skipped its scheduled run two times
skipped #3	A monitor has skipped its scheduled run three times
skipped #4	A monitor has skipped its scheduled run four times
skipped #5	A monitor has skipped its scheduled run five times
SiteScope shutting down	SiteScope has been shut down
Reached the limit of processes in the process pool	The number of processes requested from the process pool exceeds the number of processes available in the pool
Error. data reporter failed to report chunk of data	There was a fault in the transfer of SiteScope monitor measurement data to Mercury Business Availability Center
Error. config reporter failed to report chunk of data	There was a fault in the transfer of SiteScope configuration data to Mercury Business Availability Center Monitor Administration
Error. Topaz failed to process data	Mercury Business Availability Center reported a fault in processing data sent from SiteScope
Error. CacheSender. Got to the max number of cached files	SiteScope has reached the maximum number of cached data file awaiting transfer to Mercury Business Availability Center. This may occur if data transfer between SiteScope and Mercury Business Availability Center 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 Mercury Business Availability Center. This may occur if data transfer between SiteScope and Mercury Business Availability Center has been interrupted.
Topaz SEVERE	Mercury Business Availability Center reported a data transfer or processing fault with a status of `SEVERE`

Status thresholds for this monitor are set on counters listed in the table above.

Monitor Load Monitor

This monitor is designed to check several SiteScope load statistics reported by the Progress Report for the local SiteScope installation. You can edit the counters, the update frequency and the display name for this monitor type. Click **Get Counters** to edit the counters selected for the monitor. You can use the Advanced Settings disable the monitor individually as well as selecting other options as shown on the monitor properties panel.

The status thresholds for this monitor are based on the counters selected. The counters for this monitor type are listed below.

Note: Only the first 15 selected counters will be configured and monitored. A maximum of 10 measurements can be used as status threshold criteria for alerting.

Monitor Load Counters

The following are counters used for monitoring load:

- Current Monitors Run Per Minute
- Current Monitors Running
- Current Monitors Waiting

- Maximum Monitors Run Per Minute
- Maximum Monitors Running
- Maximum Monitors Waiting

Health of SiteScope Server Monitor

This monitor is designed to check the SiteScope several server resource and process statistics for the local SiteScope installation. You can edit the counters, the update frequency and the display name for this monitor type. Use the **Get Counters** link to edit the counters selected for the monitor. You can use the Advanced Settings to disable the monitor individually as well as selecting other options as shown on the monitor properties panel.

The status thresholds for this monitor are based on the counters selected. The counters available depend on the platform on which SiteScope is running. The counters for this monitor type are listed below.

Note: Only the first 15 selected counters will be configured and monitored. A maximum of 10 measurements can be used as status threshold criteria for alerting.

Health of SiteScope Server Counters on UNIX

The following are default Health of SiteScope Server Monitor counters for SiteScope on UNIX platforms:

Used Disk Space on SiteScope Drive
MegaBytes Available on SiteScope Drive
Used Disk Space on /
MegaBytes Available on /
Disk Blocks Written/sec
Disk Blocks Read/sec
Physical Memory Free
Physical Memory Free Megabytes
Swap Free,Swap Free Megabytes

Load Avg 5min
Sitescope Process Memory
SiteScope Process Thread Count
SiteScope Process Handle Count
Average CPU
PageIns/sec
PageOuts/sec
SwapIns/sec
SwapOuts/sec
ContextSwitches/sec
Net_TotalPacketsIn/sec
Net_TotalPacketsOut/sec
Net_TotalCollisions/sec

Health of SiteScope Server Counters on Windows

On the Windows platform the counters for this monitor type are presented in an expandable tree selection menu. You use the navigation features to expand and collapse the selection menu and select counters to monitor. The following are default Health of SiteScope Server Monitor counters for SiteScope on Windows platforms.

System Component	Available Counters
skipped #1	A monitor has skipped its scheduled run once
Memory	Page Faults/sec Pool Paged Bytes Pool Nonpaged Bytes % Committed Bytes In Use Available MBytes
System	Context Switches/sec File Data Operations/sec System Up Time Processor Queue Length Processes Threads

Processor	_Total % Processor Time % DPC Time
Process	java Thread Count Pool Paged Bytes Pool Nonpaged Bytes Handle Count
Process	perfex % Processor Time Thread Count Pool Paged Bytes Pool Nonpaged Bytes Handle Count
Network Interface	MS TCP Loopback interface Bytes Total/sec Current Bandwidth Bytes Received/sec Bytes Sent/sec <*Ethernet_hardware*> (hardware specific to the particular SiteScope server) Bytes Total/sec Current Bandwidth Bytes Received/sec Bytes Sent/sec
LogicalDisk	<*logical_drive*> (hardware specific to the particular SiteScope server) % Free Space Free Megabytes Avg. Disk Bytes/Transfer _Total % Free Space Free Megabytes Avg. Disk Bytes/Transfer

PhysicalDisk	_Total Current Disk Queue Length Disk Transfers/sec <*physical_disk(s)*> (hardware specific to the particular SiteScope server) Current Disk Queue Length Disk Transfers/sec
Server	Bytes Total/sec Errors Logon Errors Access Permissions Errors System Files Open Server Sessions

14

SiteScope Logs

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. These log files can be accessed using the Log Files tab. The Log Files tab is available only on the **SiteScope** root node and for the **Health** node in the monitor tree.

The following table is an overview of the log files and their content.

Log Name	Description
Alert Log	Records alert information whenever SiteScope generates an alert. This can be used to troubleshoot alert actions and to confirm that alerts were sent.
Error Log	Contains a variety of messages relating to the operation of SiteScope. This includes a record of errors that SiteScope may have encountered when trying to perform monitor actions or data communication actions. It also includes messages indicating when SiteScope was stopped or started and if there are monitors that are skipping because they are unable to complete their task.
Run Monitor Log	Records information when specific monitor runs and some actions related to managing monitors. This can be useful in troubleshooting monitors.
Mercury Business Availability Center Log	Contains information about connectivity and monitor data transfer when SiteScope is configured to report to Mercury Business Availability Center.

Log Name	Description
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. **Note:** The information in this log is only applicable to requests made to the SiteScope Classic interface.
URL Details	An optional log file used to record the complete contents of HTTP and HTTPS requests made by SiteScope URL monitor types. This can be used to troubleshoot URL and URL Sequence monitor types. This log is only enabled when the _urlDetailLogEnabled=true setting exists in the master.config file. This can be used selectively by adding the _urlDetailLogEnabled=true setting into an individual monitor group configuration file that contains a URL monitor type.
Operator Log	An optional log file used to record SiteScope operator actions, primarily information from use of the Acknowledgement feature. This log is created when an acknowledgement is added to one or more monitors.
Date Coded Monitor logs	This section contains links to the logs containing individual monitor measurements. SiteScope creates a new monitor log each day to record all monitors run during that 24 hour period. These logs are the basis for SiteScope Reports. **Note:** The monitor logs can become very large depending on the monitor environment . This may make it impractical to view them using a Web browser.

The log files are written in plain text and stored in the <SiteScope_install_path>\SiteScope\logs directory.

You use the following steps to view SiteScope logs.

To view SiteScope logs:

1. Click the **SiteScope** node in the monitor tree. Alternatively, you can click on the **Health** container in the monitor tree. The applicable view is displayed.
2. Click the **Log Files** tab in the upper right area of the contents area. The Log Files page opens.
3. Click on the name of the log file you want to view. A new browser window opens displaying the text of the log file. You can use the scroll bars to view the contents of the log or use the browser's text Find utility to locate specific information. For example, you can search for a unique text string that appears in a monitor's **Name** property to locate entries for a particular monitor instance.

Index

A

Absolute Schedules 29
  adding 31
  advanced settings 32
  settings 32
Alert log 121

C

configuration files
  enabling backups 36
  enabling use of 40

D

Database logging 43
  troubleshooting database connections 46
date format
  setting locale 35

E

e-mail
  integration with 51
E-mail Preferences
  advanced settings 57
  category settings 57
  configuring 52
E-mail Recipient Profile
  adding 55
E-mail Recipient Settings
  about 54
encoding
  enabling multiple 35
enterprise tree
  SiteScopes 6
Error log 121

G

General Settings
  configuring 33
  Suspend Monitors 39
groups
  adding to SiteScope 14

H

Health of SiteScope Server Monitor 116
  counters on UNIX 116
  counters on Windows 117

I

International version setting 35

L

license
  entering 34
  entering optional 34
Log Event Health Monitor 113
log files 121
  database table 48
  for alerts 121
  of monitor data 122
  of operator acknowledgments 122
  of post requests 122
  preferences 43
  run monitor 121
  SiteScope restarts 121
  URL monitor details 122
  viewing 123
Log Files tab 121

Log Preferences 43
settings 44

M

modem
port for pager alerts 61
Monitor Administration
SiteScope 3
Monitor Load Monitor 115
monitor logs 122
monitoring
setting domain privileges 94
SiteScope server health 107
supported Unix systems 84
monitoring remote UNIX servers 81
about 81
monitoring remote Windows servers 93
overview 100
monitors
disabling based on a schedule 70
logging data from 43
range schedules for 69
schedule to run once 29
suspending 39
troubleshooting skipped 121
troubleshooting with log files 121
using default authentication credentials for security 38

O

Operator log 122

P

pager
connection options 61
connectivity with 59
Pager Preferences
advanced settings 68
category settings 68
Pager Properties
configuring 60
Pager Recipient Profile
adding 64
testing 65
Pager Recipient Settings
about 64
Post log 122
preferences 25

R

Range Schedules
adding 71
advanced settings 74
with multiple times 71
remote servers
caching connections 99
language encoding 98
supported Unix versions 84
Unix connection methods 85
Unix language encoding 87
Windows connection methods 97
remote Windows server profiles
about 94
adding 95
reports
log files used by 122
Run Monitor log 121

S

security
using default authentication credentials 38
setting Log Preferences 44
SiteScope 3
adding groups 14
adding to enterprise tree 6
attaching 20
configuration data files 40
data logging options 43
deleting 20
detaching 20
editing settings 13
managing in Monitor Administration 3
replicating configuration settings 19
SNMP Preferences 75
SiteScope Absolute Schedule Preferences 29
SiteScope E-mail Preferences 51

SiteScope General Settings 33
SiteScope Health 107
  adding monitors 108
  Health of SiteScope Server Monitor 116
  Log Event Health Monitor 113
  log events 109
  log files 121
  monitor group 107
  monitor load 111
  Monitor Load Monitor 115
  monitor reference 113
  server health 112
  understanding 109
SiteScope log database table 48
SiteScope Pager Preferences 59
SiteScope Preferences 25
SiteScope profiles 6
SiteScope Range Schedule Preferences 69
SNMP
  configuring SiteScope properties 76
  defining multiple profiles 78
  integration with 75
SNMP Preferences
  about 75
  advanced settings 80
SNMP Recipient Profile
  adding 78
SNMP Recipient Settings 77
SNMP trap settings 75
suspending monitor processes 39

T

time format
  setting locale 35
troubleshooting
  database connections 46
  Trace UNIX connections 84

U

Unix
  secondary prompt for telnet 86
  supported for monitoring 84
UNIX Servers
  advanced settings 87
UNIX servers
  adding 82
  technical notes on monitoring 89
URL details log 122
URL Monitor
  using default authentication credentials for security 38

W

Windows servers
  about monitoring remote 93
  advanced settings 98
  main settings 96
  monitoring remote 93
  perfex for troubleshooting connections 102
  technical notes on monitoring 100
  troubleshooting event log access 101