OPTIMIZE

MERCURY BUSINESS AVAILABILITY CENTER™

SiteScope Administration

MERCURY™

BUSINESS TECHNOLOGY OPTIMIZATION

Mercury Business Availability Center

SiteScope Administration

Version 6.1

Document Release Date: March 5, 2006

MERCURY™

Mercury Business Availability Center, Version 6.1
SiteScope Administration

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

© 2005-2006 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_SISADM6.1/01

Table of Contents

Welcome to SiteScope Administration ..... **v**
How This Guide Is Organized v
Who Should Read This Guide vi
Getting More Information vi

PART I: INSTALLING SITESCOPE

Chapter 1: Introducing and Deploying SiteScope **3**

Chapter 2: Before You Install SiteScope **5**
System Requirements and Sizing Recommendations 5
Preparing to Upgrade an Existing SiteScope Installation 10
Registering for SiteScope Support 13

Chapter 3: Installing SiteScope on Solaris or Linux **15**
Preparing for Installation on Solaris or Linux 15
Installing SiteScope 16
Connecting to SiteScope 34

Chapter 4: Installing SiteScope for Windows **41**
Installing SiteScope on Windows Platforms 41
Connecting to SiteScope on Windows Platforms 50

Chapter 5: Copying SiteScope Configurations **55**

Chapter 6: Uninstalling SiteScope **61**
Uninstalling SiteScope for Windows Platforms 61
Uninstalling SiteScope for Solaris or Linux 63

PART II: RUNNING SITESCOPE SECURELY

Chapter 7: Hardening the SiteScope Platform **71**

Chapter 8: Configuring SiteScope to Use SSL **73**
About Using SSL in Mercury SiteScope 73
Preparing SiteScope for Using SSL 74
Configuring SiteScope 8.0 and Later for SSL 78
Configuring SiteScope Classic for SSL 80

PART III: EXTERNAL INTEGRATIONS AND FUNCTIONALITY

Chapter 9: Integration with Mercury Business Availability Center....85
Understanding SiteScope Integration with Mercury Business Availability Center Products 86
Registering SiteScope to Mercury Business Availability Center....90
Changing the Core Server to Which SiteScope Sends Data....95
Setting Up the Mercury Self-Alert Monitor Group 99
Using SSL for SiteScope-Mercury Business Availability Center Communication 99
Reporting Status per Measurement 101
Troubleshooting Data Reporting to Mercury Business Availability Center 102

Chapter 10: Integrating SiteScope with Mercury Managed Services 103
Understanding SiteScope Integration with Mercury Managed Services. 104
Registering SiteScope to Mercury Managed Services 105

Chapter 11: Integrating SiteScope with Mercury SiteSeer 109
Understanding Integration with Mercury SiteSeer 110
Settings for SiteSeer Integration 111

Chapter 12: Mercury Self-Alert Monitor....115
Understanding the Mercury Self-Alert Monitor Group 115
Working with the Mercury Self-Alert Monitor Group....117
Mercury Self-Alert Monitor Templates....122
Mercury Self-Alert Monitor Troubleshooting 125
Troubleshooting Directory and Log File Errors....126

Chapter 13: Host Last Connection Time Monitor 135
Understanding the Host Last Connection Time Monitor 135
Configuring the Host Last Connection Time Monitor....136

Chapter 14: Host Last Reported Data Time Monitor 141
Understanding the Host Last Reported Data Time Monitor 141
Configuring the Host Last Reported Data Time Monitor....142

Index....149

Welcome to SiteScope Administration

This guide provides detailed instructions on how to deploy SiteScope and integrate the SiteScope data collector into Mercury Business Availability Center.

How This Guide Is Organized

The guide contains the following chapters:

Part I Installing SiteScope

Introduces the SiteScope data collector and details the process of installing, accessing, upgrading, and uninstalling SiteScope on Windows and Unix operating systems.

Part II Running SiteScope Securely

Describes steps to take to secure the SiteScope application and platform.

Part III External Integrations and Functionality

Describes how SiteScope can be integrated with other Mercury Business Availability Center applications.

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, scripting, and Mercury Business Availability Center data collectors.

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

Installing SiteScope

1

Introducing and Deploying SiteScope

SiteScope is a real-time status and alerting solution for monitoring IT system availability. Its agentless monitoring architecture enables you to monitor your network environment without the having to deploy agent software onto the servers to be monitored. This makes deployment and maintenance of SiteScope more efficient compared to other system or operational monitoring solutions.

SiteScope is a versatile operational monitoring solution with over 80 ready-made monitor types for monitoring a wide variety of systems and services at different levels. This includes monitoring basic server resources, performance metrics from applications, and the availability of end-user services. See "Working with SiteScope Monitors" in *Configuring SiteScope Monitors* for more information. Many of the monitor types can be customized for special environments. Templates provide a tool for developing standardized monitoring organization and speeding monitor deployment. See "Using Templates to Deploy Monitors" in *Configuring SiteScope Monitors* for more information.

SiteScope includes nine standard alert types that you can use to communicate and record event information in a variety of media. You can customize alert templates to meet the needs of your organization. See "Introducing SiteScope Alerts" in *Configuring SiteScope Alerts* for more information.

SiteScope is licensed on the basis of the number of metrics to be monitored rather than the number of servers on which it is run. A metric is a system resource value, performance parameter, URL, or similar system response. This means that you can flexibly scale a SiteScope deployment to meet the needs of your organization and the requirements of your infrastructure. You can install SiteScope using either a permanent license that you receive from Mercury or the evaluation license that is part of a new SiteScope installation. You can upgrade your licensing as needed to expand the monitoring capacity of your initial deployment or to expand the deployment within your infrastructure. For more information on SiteScope licenses, refer to *Getting Started with SiteScope* in the *SiteScope Help*.

2

Before You Install SiteScope

SiteScope is a standalone application with an agentless architecture that is designed to be rapidly deployable. There are several planning steps and actions you should consider before you install SiteScope to facilitate the deployment and management of your monitoring environment.

This chapter describes:	On page:
System Requirements and Sizing Recommendations	5
Preparing to Upgrade an Existing SiteScope Installation	10
Registering for SiteScope Support	13

System Requirements and Sizing Recommendations

Below are the minimum system requirements and recommendations for running SiteScope, based on the various supported operating systems. The table of Recommended Configurations is a guide for sizing a server for deployment of SiteScope in a production environment.

System Requirements for Windows

Use these system requirements when installing SiteScope on Windows platforms.

Computer/Processor	Pentium III, 800 MHZ or higher
Operating System	Microsoft Windows 2000 SP4, or 2003 Server
Memory	512 MB minimum (2 GB+ recommended)
Free Hard Disk Space	2 GB or more (10 GB+ recommended)
Web Browser	Microsoft Internet Explorer 6.0 SP1 or later; Firefox 1.0 or later

System Requirements for Solaris

Use these system requirements when installing SiteScope on Solaris.

Computer/Processor	Sun 400 MHz UltraSparc II Processor or higher
Operating System	Sun Solaris 2.8, 2.9, or 2.10
Memory	512 MB minimum (2 GB+ recommended)
Free Hard Disk Space	2 GB or more (10 GB+ recommended)
Web Browser	Firefox 1.0 or later

Note: To view SiteScope Management Reports on UNIX based machines, it is necessary that an X Window system be running on the server where SiteScope is running.

System Requirements for RedHat Linux

Use these system requirements when installing SiteScope on RedHat Linux.

Computer/Processor	Pentium III, 800 MHZ or higher
Operating System	RedHat Linux 9.0 with Native POSIX Threading Library (NPTL) , or RedHat Enterprise Linux 2.0 or 3.0
Memory	512 MB minimum (2 GB+ recommended)
Free Hard Disk Space	2 GB or more (10 GB+ recommended)
Web Browser	Firefox 1.0 or later

Recommended Configurations

The following table contains recommended server configurations for SiteScope deployments. These are general recommendations based on the number of monitor instances configured and how many monitors are run per minute on the SiteScope server.

Level	Sever Description	Intel Platform	Solaris Platform
1	A SiteScope server with fewer than 1000 monitors and less than 300 monitors/minute running.	Single Processor (Pentium III 1.0 GHz or higher)*, 512 MB System Memory, Single Network Controller, 2 GB disk space.	Single Processor (for example, Ultra 10/Netra T1), 512 MB System Memory, Single Network Controller, 2 GB disk space.

Level	Sever Description	Intel Platform	Solaris Platform
2	A SiteScope server running between 1000 and 2000 monitors, and less than 500 monitors/minute running.	Dual Processor (Pentium III 1.0GHz/Pentium III 700 MHz Xeon or higher)*, 1024 MB System Memory, Dual Network Controllers with Fast Ethernet, 4 GB disk space.	Dual Processors (Ultra 2/E220/E250 400 MHz+), 784 MB System Memory, Dual Network Controller with Fast Ethernet, 4 GB disk space.
3	A SiteScope server with more than 2000, but less than 4000 monitors, and more than 500 monitors/minute running.	Quad Processor (Pentium III Xeon 700 MHz or higher)*, 1024-1536 MB System Memory, at least Dual Network Controller with Fast Ethernet, 8 GB disk space.	Dual Processor (E280r) or Quad Processor (Ultra2/E220/E250), 1024 MB System Memory, at least Dual Network Controller with Fast Ethernet, 8 GB disk space.

* Dual or multiple processor systems are more beneficial for SiteScope performance than simply increasing processor speed. Intel Xeon Processors are recommended for Level II and Level III implementations as applicable.

Note: It is recommended that any SiteScope implementation having more that 4000 individual monitor instances be divided across multiple SiteScope installations on separate servers.

Additional Considerations for SiteScope Server Sizing

The following are additional considerations and recommendations for sizing a server for SiteScope deployment and performance.

- Using high speed (10K/15K RPM) SCSI disk drives can help improve SiteScope system I/O.
- When monitoring across WAN/slow network links, the network will usually become the bottleneck. This can require additional time for the monitor(s) to execute.
- When enabling SiteScope Database Logging or Mercury BAC Logging (for example, having SiteScope report as an agent to Mercury Business Availability Center or Mercury Managed Services), add dual processor support if the total number of monitor instances approaches or exceeds 700 monitors.
- When using high frequency monitoring (monitoring more frequently than once every minute) using Ping, Win NT, or UNIX Telnet (for Server monitors), add more processor support, such as additional processors and higher processor speed. This is necessary to handle the increased I/O and process forking.

Preparing to Upgrade an Existing SiteScope Installation

SiteScope is designed for backward compatibility. This means you can install newer versions of SiteScope and transfer monitor configurations from an existing SiteScope installation with a minimum of disruption to monitoring function. However, because of the many ways that SiteScope can be customized, it is recommended that you install newer versions of SiteScope in a clean directory structure and make a backup copy of key SiteScope data before upgrading.

Note: Before installing SiteScope 8.1, you must have SiteScope 8.0 installed. You must install SiteScope 8.1 into the same directory as SiteScope 8.0. If you are installing SiteScope 8.0, you must create a new directory for installation of SiteScope 8.0. Do not install version 8.0 into a directory used for a previous version of SiteScope.

The new directory you create for installing SiteScope must be named SiteScope and be located in a different directory path. For example, if the original SiteScope directory was C:\SiteScope, the new directory could be C:\8.0\SiteScope.

After installation, monitor configuration data can be copied from the earlier version to SiteScope 8.0 and 8.1 using the copy utility. See "Copying SiteScope Configurations" for more information.

The simplest way to prepare for a SiteScope upgrade is to make a backup of your current SiteScope installation directory and all of the subdirectories within the directory.

Important: Beginning with version 8.0.0.0, SiteScope incorporates a new, binary configuration storage scheme. When upgrading from a version earlier than 8.0.0.0, the configuration data in the monitor group files will be read and copied into the new configuration data storage. When you upgrade from an earlier SiteScope version, you must resolve any monitor group and master configuration file errors before you copy those files to the new SiteScope installation. You can use the SiteScope Health monitoring features in earlier versions of SiteScope to check for configuration file errors. For details, see "Monitoring SiteScope Server Health" in *Managing SiteScope*.

SiteScope daily monitor logs may require a large amount of storage space for backup depending on the number of monitors configured, the frequency of monitor runs, and the number of days that data logs are maintained. If it is not practical to make a complete backup of the SiteScope installation directory, it is highly recommended that you make a backup of the contents of the following directories from your current SiteScope installation.

Directory	Description
SiteScope\groups	Contains monitor, alert, report, and other critical configuration data needed for SiteScope operation.
SiteScope\scripts	Contains scripts used by Script monitors.
SiteScope\scripts.remote	Contains command scripts used by Script monitors to trigger other scripts on remote servers.
SiteScope\templates.*	Includes data and templates used to customize monitor function, alert content, and other features. The group of subdirectories all begin with the name templates (for example, templates.mail, templates.os, templates.page).

Directory	Description
SiteScope\htdocs	Contains scheduled reports and user-customized style sheets for the SiteScope interface.
SiteScope\conf\ems	Contains key configuration and control files used with Integration monitor types. This is only applicable if you use SiteScope as an agent reporting to another Mercury Business Availability Center application.

The SiteScope\logs directory contains a number of logs including date-coded logs of monitoring data. The total storage space used by these log files may be much larger than the files that comprise the SiteScope software. You may decide to selectively back up the most recent monitoring data log files along with the other log types in this directory. For example, make a backup of the last seven days of monitoring data logs. The log files containing monitor measurements are date-coded files with a filename of the following format:

SiteScopeyyyy_mm_dd.log

You can selectively backup these log files beginning with the most recently created files.

You may also want to backup the following logs for historical continuity:

- error.log
- RunMonitor.log
- access.log
- alert.log
- monitorCount.log
- EmsMonitors.log

Registering for SiteScope Support

Register your copy of SiteScope to become a licensed user with all applicable rights and privileges. Registered users can access technical support and information on all Mercury products and are eligible for updates and upgrades. You will also be given access to the Mercury Customer Support Web site. You can use this access to search for technical information in the SiteScope Knowledge Base as well as downloading printer-friendly versions of the SiteScope documentation.

Note: You can register your copy of SiteScope on the Mercury Customer Support Web site (http://support.mercury.com).

If your address changes, notify Mercury or your local representative so that you can continue to receive product information and updates.

3

Installing SiteScope on Solaris or Linux

SiteScope for Solaris and SiteScope for Linux are available as a single, compressed archive file that can be downloaded from the Mercury Web site. It is also available on CD-ROM. SiteScope is installed on a single server and runs as a single application or process. This means you can install SiteScope in minutes and begin monitoring your systems and servers.

This chapter describes:	On page:
Preparing for Installation on Solaris or Linux	15
Installing SiteScope	16
Connecting to SiteScope	34

Preparing for Installation on Solaris or Linux

Depending on your environment, preparation for installation of SiteScope on UNIX or Linux involves creating a user login account, selecting a suitable installation location, and setting account permissions.

To prepare for installation of SiteScope on UNIX or Linux:

1. Create a user account that will be used to run the SiteScope application. Set the default shell for the account.
2. Select or create an installation location for the SiteScope application, for example, /opt/, /usr/local/SiteScope, or /home/monitoring/SiteScope. Verify that the installation location has access to sufficient disk space for the installation and operation of SiteScope.

Important: Before installing SiteScope 8.1, you must have SiteScope 8.0 installed. You must install SiteScope 8.1 into the same directory as SiteScope 8.0. If you are installing SiteScope 8.0, you must create a new directory for installation of SiteScope 8.0. Do not install version 8.0 into a directory used for a previous version of SiteScope.

---

3 Set the permissions for the SiteScope installation directory to have read, write, and execute permissions for the user account that will be used to run the SiteScope application. The permissions must also be set for all subdirectories within the SiteScope installation directory.

Note: While SiteScope does require highly privileged account permissions to enable the full range of server monitoring, it is recommended not to run SiteScope from the root account and not to configure SiteScope to use the root account to access remote servers.

Installing SiteScope

Beginning with version 7.8.1.2, SiteScope for Solaris and SiteScope for Linux include several installation options. The options are:

- multi-platform installation executable with an interactive graphical user interface (for details, see "Installing SiteScope Using the Installation Executable" on page 17)
- console mode installation script using command line inputs (for details, see "Installing SiteScope Using Console Mode" on page 26)
- automated, non-interactive installation using a template file (for details, see "Installing SiteScope Using an Installation Template" on page 33)

Installing SiteScope Using the Installation Executable

You can install SiteScope on Solaris or Linux using the multi-platform InstallShield wizard.

Note: The multi-platform InstallShield wizard automatically executes if X11 libraries have already been installed on the server. If these libraries are not installed, install SiteScope in console mode. For information, see "Installing SiteScope Using Console Mode" on page 26

Use the following steps to install SiteScope using the installation executable.

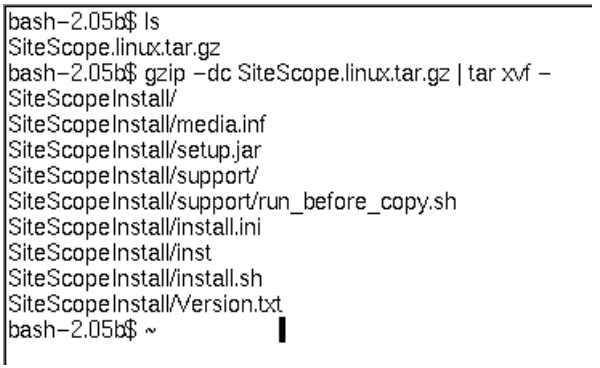
To install SiteScope on Solaris or Linux using the multi-platform installer:

1. Download the SiteScope compressed archive file on the machine where you want to install SiteScope. Alternatively, insert the CD-ROM with the SiteScope software into the CD-ROM drive.
2. Copy the SiteScope compressed archive file to a disk or network location where it is accessible to the user account that is to be used to install SiteScope.
3. Decompress and extract the SiteScope files from the compressed archive with the following command:

   gzip -dc SiteScope.*system*.tar.gz | tar xvf -

   Replace system with the platform name included as part of the compressed archive filename (the choices are sun or linux). The decompression and archive extraction process are displayed on the standard output.

An example of the extraction command and results is shown in the figure below.

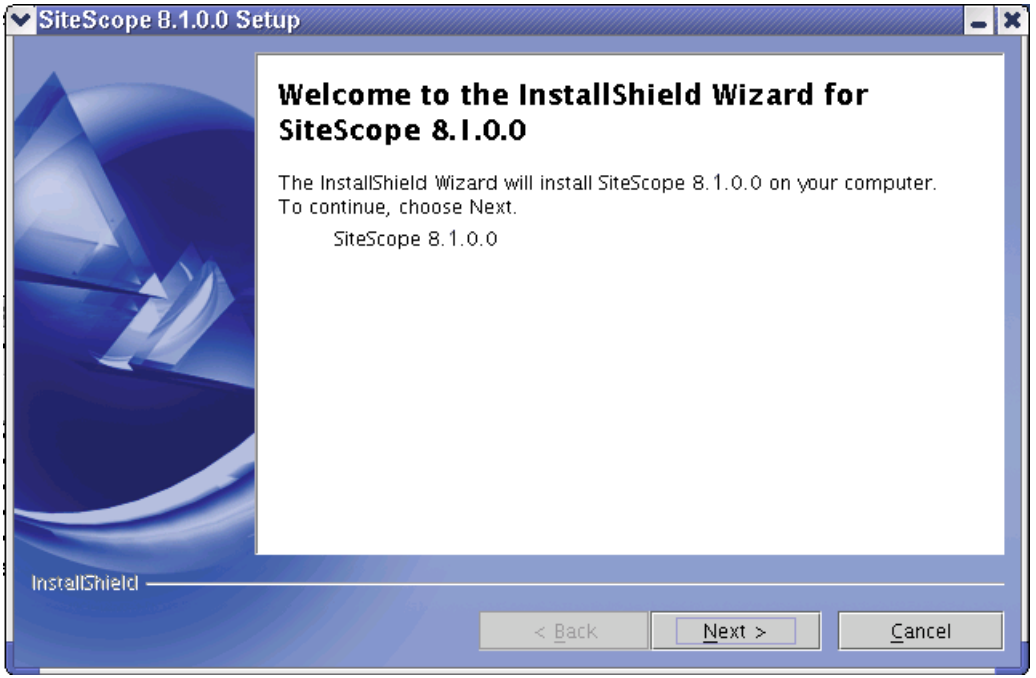


The extraction operation creates a new directory called SiteScopeInstall that contains the files used for the installation.

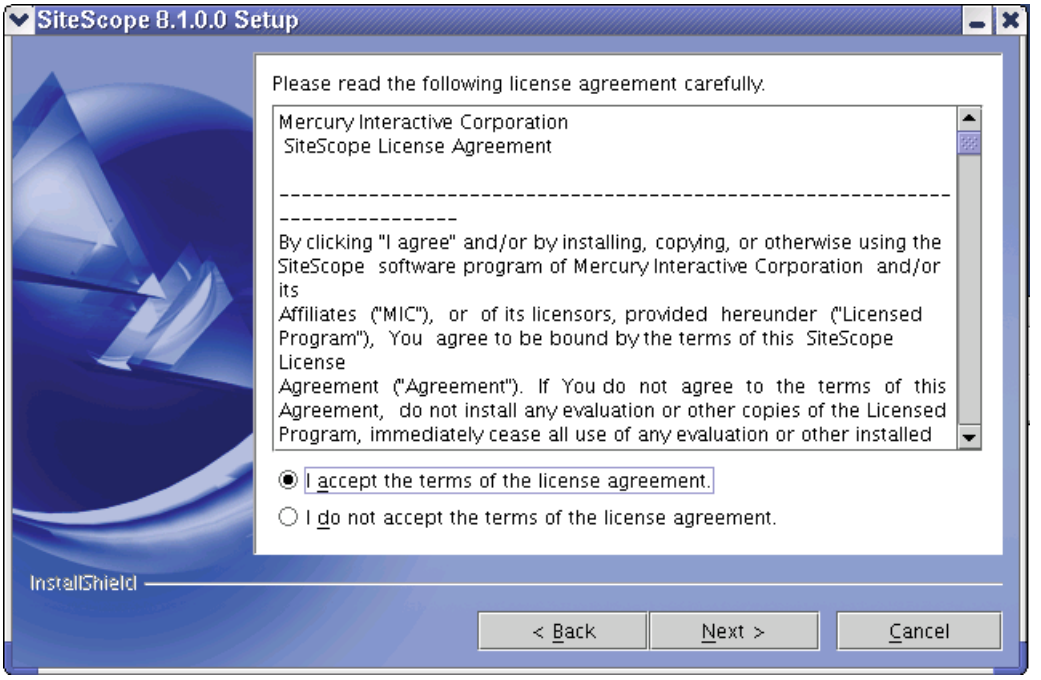
4 Run the installation script found in the SiteScopeInstall directory with the following command:

SiteScopeInstall/inst

The installation executable initializes the InstallShield wizard and the Java Virtual Machine. The InstallShield Welcome window opens.



5 Click **Next** to continue. The SiteScope Software License Agreement screen opens.



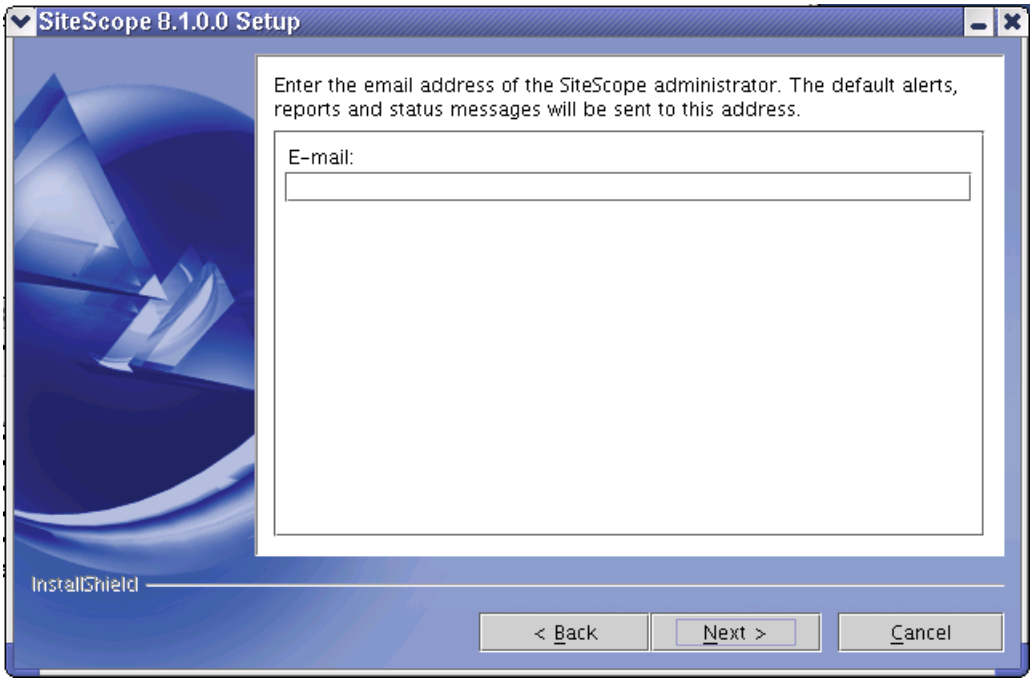
6 Read the SiteScope License Agreement.

To install SiteScope, you must accept the terms of the license agreement.

After you install SiteScope, the text of the SiteScope license agreement can be found in the file <SiteScope root folder>/license.html.

7 Click **I accept** button to confirm that you accept the Software License Agreement and then click **Next** to continue. The Administrator E-mail Address screen opens.

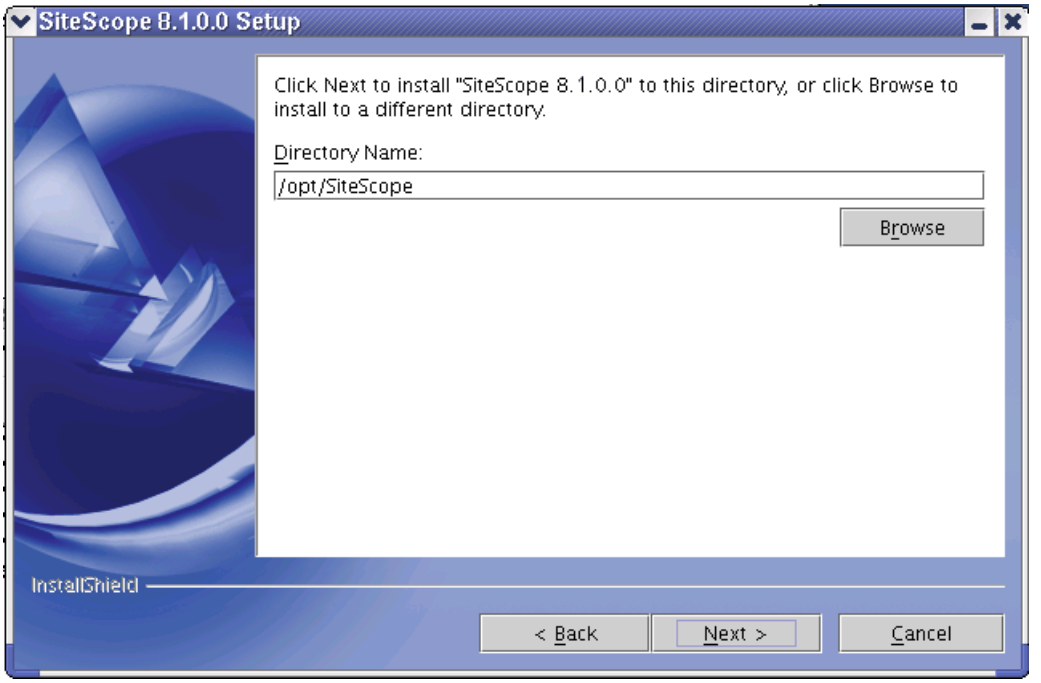
8 Enter the e-mail address that SiteScope should use to send e-mail alerts to the SiteScope administrator.



Note: Entering an e-mail address at this step is not mandatory for the installation of SiteScope. You can enter this information later using the E-mail Preferences page in SiteScope.

---

9 Click **Next** to continue. The Installation Directory Selection screen opens.



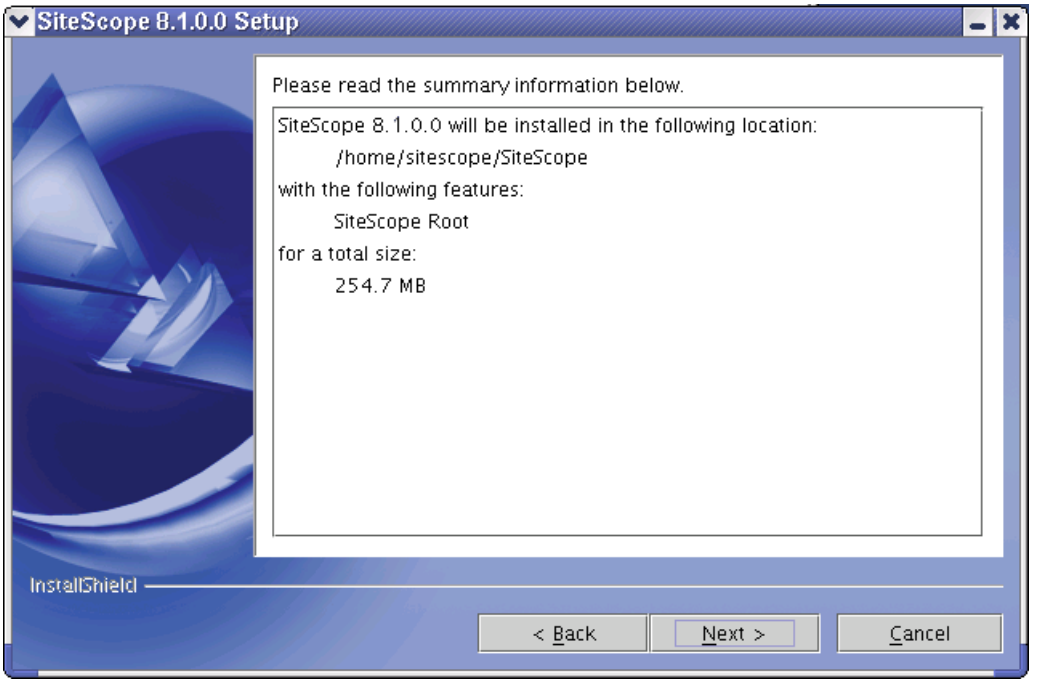
10 Select the directory where you want SiteScope to be installed.

- Click **Next** to accept the default install path as displayed.
- Click **Browse** to change the installation location.

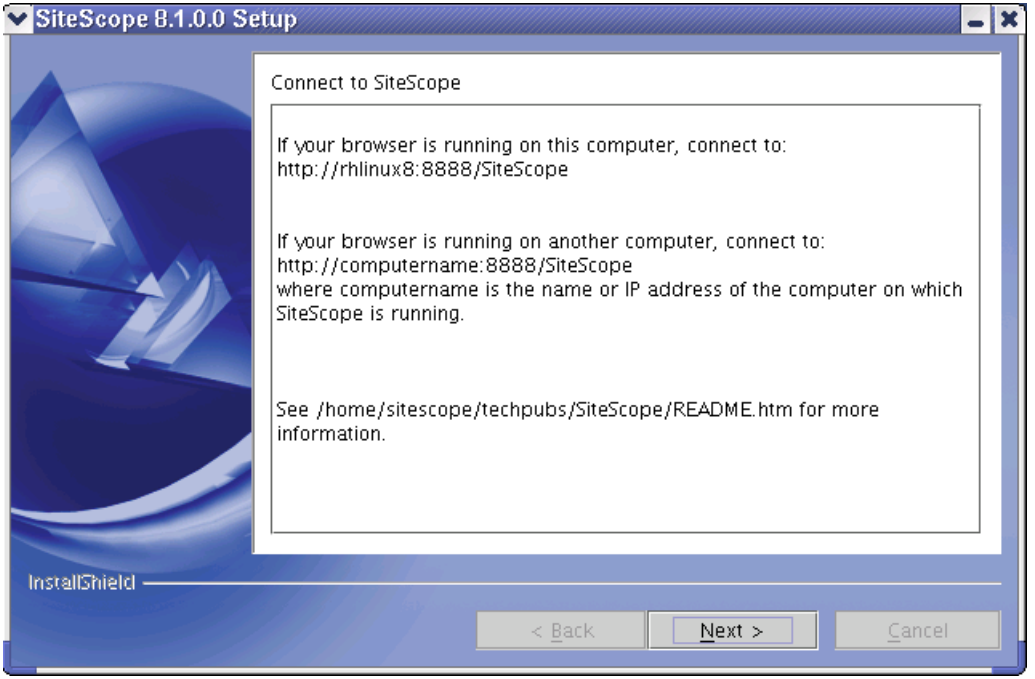
Important: Before installing SiteScope 8.1, you must have SiteScope 8.0 installed. You must install SiteScope 8.1 into the same directory as SiteScope 8.0. If you are installing SiteScope 8.0, you must create a new directory for installation of SiteScope 8.0. Do not install version 8.0 into a directory used for a previous version of SiteScope.

---

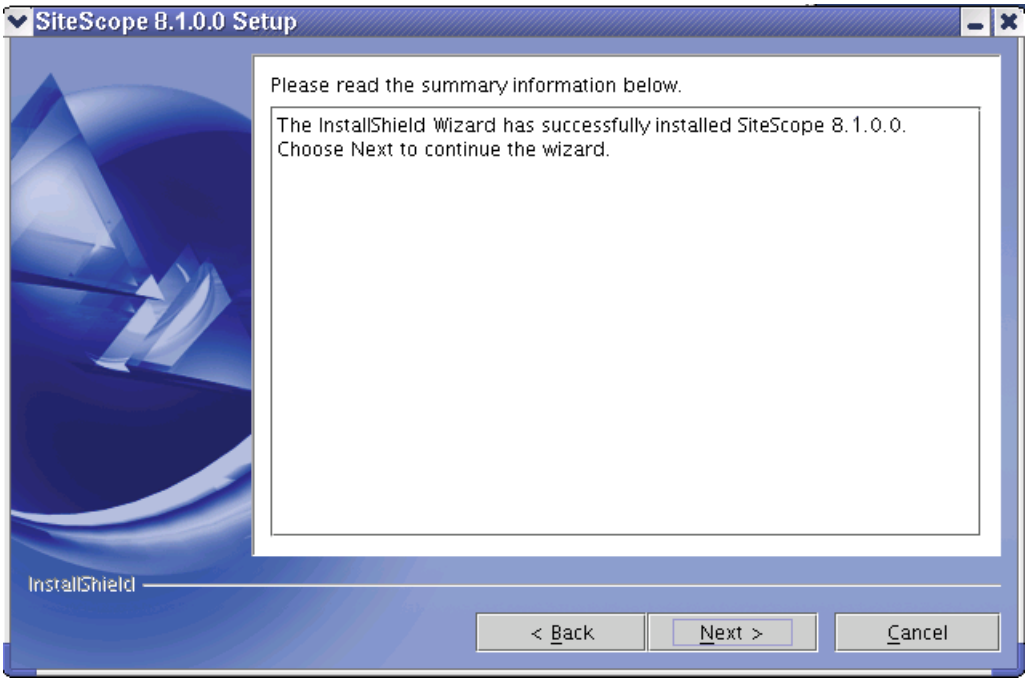
11 Click **Next** to continue. The Summary Information screen opens.



12 Click **Next** to accept the installation settings. The SiteScope installation process starts. An installation progress screen opens. When the installation process is complete, the SiteScope process starts and the Connect to SiteScope screen opens.



Make a note of the information for connecting to SiteScope. Click **Next** to continue. The installation completion screen opens.



13 Click **Next** to complete the installation process and close the InstallShield wizard. To deploy SiteScope, follow the steps in the section "Connecting to SiteScope" on page 34.

14 For the latest available functionality, download the latest service pack from the same location from which you installed SiteScope. Install the service pack into the same directory as SiteScope.

Installing SiteScope Using Console Mode

You can install SiteScope using a command line or console mode. You use this option if you are installing SiteScope on a remote server or for any other reason that prevents the use of the installation option via the user interface.

To install SiteScope on Solaris or Linux using the console mode:

1. Download the SiteScope compressed archive file, or insert the CD-ROM with the SiteScope software into the CD drive, on the machine where you want to install SiteScope.
2. Copy the SiteScope compressed archive file to a disk or network location where it is accessible to the user account that is to be used to install SiteScope.
3. Decompress and extract the SiteScope files from the compressed archive by running the following command:

   gzip -dc SiteScope.*system*.tar.gz | tar xvf -

   Replace *system* with the platform name included as part of the compressed archive filename (the choices are sun or linux). The console displays the decompression and archive extraction process as shown below.

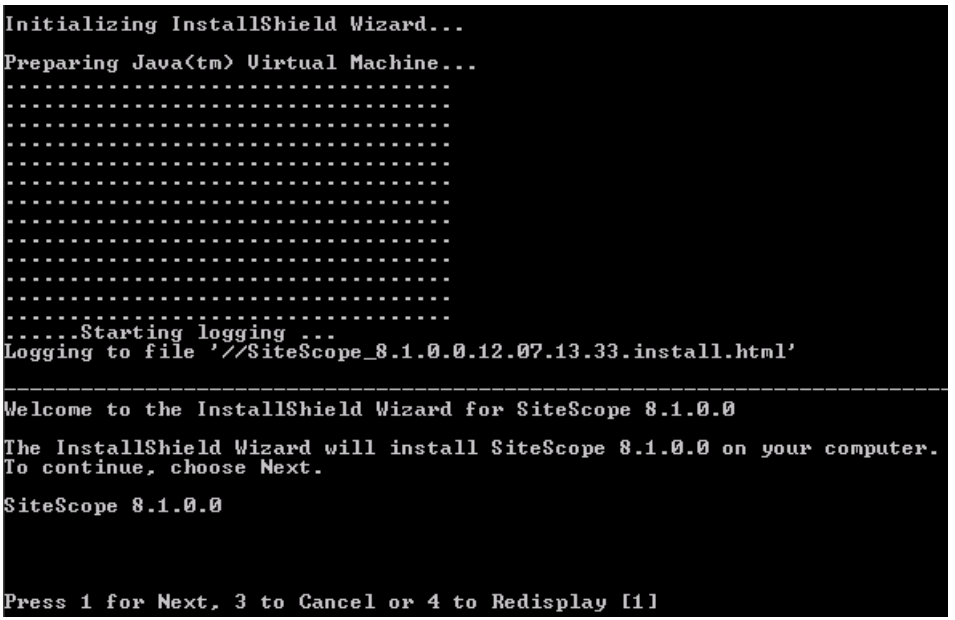
```
bash-2.05b$ ls
SiteScope.linux.tar.gz
bash-2.05b$ gzip -dc SiteScope.linux.tar.gz | tar xvf -
SiteScopeInstall/
SiteScopeInstall/media.inf
SiteScopeInstall/setup.jar
SiteScopeInstall/support/
SiteScopeInstall/support/run_before_copy.sh
SiteScopeInstall/install.ini
SiteScopeInstall/inst
SiteScopeInstall/install.sh
SiteScopeInstall/Version.txt
bash-2.05b$ ~
```

   The operation creates a new directory named /SiteScopeInstall. This directory contains the installation executable and other files used to install SiteScope.

4 After the SiteScope software files have been extracted, run the installation script supplied with SiteScope with the following command:

```
/bin/sh SiteScopeInstall/install.sh -console
```

The installation script initializes the Java Virtual Machine to begin the installation. A confirmation screen is displayed.



5 Enter the number 1 to continue with the installation. The text of the license agreement is displayed. To cancel the installation before reading the license agreement, enter the number 3 and then confirm that you want to cancel the installation.

```
Press 1 for Next, 3 to Cancel or 4 to Redisplay [1] 1

-------------------------------------------------------------
Please read the following license agreement carefully.

Mercury Interactive Corporation
 SiteScope License Agreement
 -------------------------------------------------------------
By clicking "I agree" and/or by installing, copying, or otherwise using the
SiteScope  software program of Mercury Interactive Corporation  and/or  its
Affiliates  ("MIC"),  or  of its licensors, provided  hereunder  ("Licensed
Program"),  You  agree to be bound by the terms of this  SiteScope  License
Agreement  ("Agreement").  If  You do  not  agree  to  the  terms  of  this
Agreement,  do not install any evaluation or other copies of the Licensed
Program, immediately cease all use of any evaluation or other installed copies
of the Licensed Program, and remove from Your system computers and destroy any
and all such copies and any associated documentation downloaded by You or
provided from MIC ("Documentation").

MIC, or its licensors, owns all intellectual property rights in and to  the
Licensed  Program  and  Documentation, including patent,  copyright,  trade
secret, trademark and other proprietary rights. Your rights are limited  to
those  expressly  granted in this Agreement. This Agreement  grants  You  a
nontransferable and non-exclusive license to use, solely for Your  internal
business  purposes, the Documentation and the object code  version  of  the

Press ENTER to read the text [Type q to quit]
```

The SiteScope License Agreement requires several pages to display. Read each page as it is presented. Press ENTER to continue to the next page. When you have viewed all the pages of the license agreement, you have the option to accept or not accept the license agreement.

```
Press ENTER to read the text [Type q to quit]

used in this Agreement are provided for convenience only, and shall not  in
any  way affect the meaning or interpretation hereof. A waiver of a  breach
or  default under this Agreement shall not be a waiver of any other  breach
or default.  Failure of either party to enforce compliance with any term or
condition of this Agreement shall not constitute a waiver of such  term  or
condition unless accompanied by a clear written statement that such term or
condition  is  waived.  MIC will  not be responsible  for  any  failure  to
perform  due  to  "force  majeure" causes  beyond  its  reasonable  control
including,  but  not  limited to, acts of God, riots, embargoes,  terrorist
acts,  acts  of civil or military authorities, disruptions in the  flow  of
data  to  or  from  networks, denial of or delays in processing  of  export
license applications, accidents, strikes, fuel crises or power outages.

Mercury Interactive, the Mercury Interactive logo, and all other trademarks
which  identify  the  Licensed  Program are the  trademarks,  and  in  some
jurisdictions may be registered trademarks, of Mercury Interactive  or  its
affiliates.  All other company, brand and product names are the  trademarks
of their respective holders

(c) copyright 2004 Mercury Interactive Corporation. All rights reserved.

Please choose from the following options:

[ ] 1 – I accept the terms of the license agreement.
[X] 2 – I do not accept the terms of the license agreement.

To select an item enter its number, or 0 when you are finished: [0]
```

To install SiteScope, you must accept the terms of the license agreement. The default selection is to not accept the agreement. To accept the license agreement and continue the installation, enter the number 1 and then enter the number zero (0) to continue. A continuation prompt is displayed.

Note: To cancel the installation after viewing the SiteScope License Agreement, enter the number 1, enter the number zero, and then enter the number 3 at the next continuation prompt to cancel the installation.

---

6 Enter 1 to continue the installation process. The E-mail address entry prompt is displayed.

```
[X] 1 – I accept the terms of the license agreement.
[ ] 2 – I do not accept the terms of the license agreement.

To select an item enter its number, or 0 when you are finished: [0] 0


Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1] 1

--------------------------------------------------
Enter the email address of the SiteScope administrator. The default alerts,
reports and status messages will be sent to this address.

E-mail: []
```

7 Enter a SiteScope administrator e-mail address. For example, sitescopeadmin@thiscompany.com. If you do not want to enter an e-mail address at this time, press ENTER to leave this blank and continue to the next step. You can enter e-mail information later using the E-mail Preferences page once SiteScope is running

8 Enter 1 to continue to the next step. The Installation Location selection prompt is displayed.

```
SiteScope 8.1.0.0 Install Location

Please specify a directory or press Enter to accept the default directory.

Directory Name: [/opt/SiteScope]
```

9 Enter the location where you want to install SiteScope. The default location is shown between square brackets and is relative to the location of the installation executable. To enter a different installation location, type the location path as a command line entry without square brackets. The installation location must end with a directory called SiteScope.

10 Enter 1 to continue with the installation. The console displays the installation parameters for confirmation.

```
---------------------------------------------------
SiteScope 8.1.0.0 will be installed in the following location:

/home/sitescope/SiteScope

with the following features:

SiteScope Root

for a total size:

 254.7 MB

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
```

11 Enter 1 to proceed with the installation using the installation location indicated. Enter 2 to return to the previous dialogue and make changes. The installation process starts. When the installation is completed, SiteScope starts and the Connect to SiteScope screen is displayed.

```
-------------------------------------------------------------
Connect to SiteScope


If your browser is running on this computer, connect to:
http://rhlinux8:8888/SiteScope


If your browser is running on another computer, connect to:
http://computername:8888/SiteScope
where computername is the name or IP address of the computer on which SiteScope
is running.



See /home/sitescope/techpubs/SiteScope/README.htm for more information.

Press 1 for Next or 4 to Redisplay [1]
```

At this point, SiteScope is installed and running.

12 Make a note of the SiteScope address and port number displayed on the screen. By default, SiteScope will try to answer on port 8888. If another application is using that port number, SiteScope will try another port number (for example port 8889). To connect to SiteScope, follow the steps in the section "Connecting to SiteScope" on page 34.

13 Enter 1 to continue to the next step. An installation status message is displayed. Enter 1 to exit the installation script.

```
-------------------------------------------------------------
The InstallShield Wizard has successfully installed SiteScope 8.1.0.0. Choose
Next to continue the wizard.

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
```

14 For the latest available functionality, download the latest service pack from the same location from which you installed SiteScope. Install the service pack into the same directory as SiteScope.

Installing SiteScope Using an Installation Template

You can automate the installation of SiteScope on UNIX and Linux platforms by creating an installation template and then using that template to provide inputs requested by the installer. Use this method in combination with other system scripts to automatically install SiteScope in multiple locations or as part of a scheduled task.

To create a SiteScope installation template:

1 Create a template file to be used for automated installation by running the install script with the following options:

```
SiteScopeInstall/install.sh -console -options-template ./install.tmp
```

Note: The syntax of this command line includes a space before the -console option and the -options but no space before the -template argument.

This creates a template file called install.tmp in the /SiteScopeInstall directory.

2 Open the template file with a text editor.

3 Edit the template file for your environment. The template file itself provides documentation on how to modify it. The three parameter values that you will need to specify in the template for SiteScope installation are:

- the value for accepting the software license agreement (set the value equal to 1 to accept the license agreement)
- the SiteScope administrator's e-mail address (for example: sitescopeadmin@thiscompany.com)
- the installation path for SiteScope (for example: /usr/local/SiteScope)

Note: The installation path must end with a directory called SiteScope.

To install SiteScope using the installation template:

1. Download the SiteScope installation package to the machine or machines where you want to install it.
2. Decompress the SiteScope installation package into the directory where you want to install the software. This will create a /SiteScopeInstall subdirectory.
3. Copy the installation template into the /SiteScopeInstall subdirectory.
4. Execute the SiteScope installation script and pass in the template file with the following command syntax:

   ```
   SiteScopeInstall/inst -silent -options ./install.tmp
   ```

   Note: This command invokes the installer executable and not the install shell script, install.sh.

   SiteScope will now be installed silently using the template file to answer all the inputs requested by the installer.
5. For the latest available functionality, download the latest service pack from the same location from which you installed SiteScope. Install the service pack into the same directory as SiteScope.

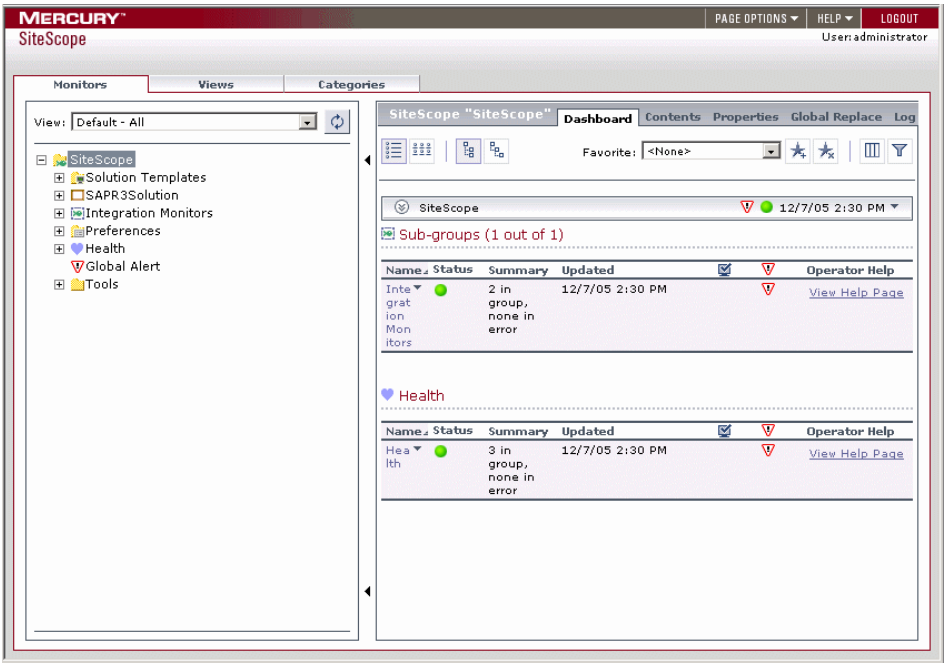
Connecting to SiteScope

SiteScope is designed as a Web application. This means that you view and manage SiteScope using a Web browser with access to the SiteScope server.

SiteScope is installed to answer on two ports: 8080 and 8888. If there is another service configured to use these ports, the installation process attempts to configure SiteScope to answer on another port. SiteScope updates the port number information in the file Open SiteScope.htm. This file is an HTML page that is found in the SiteScope installation directory. The following section describes how to connect to SiteScope.

Accessing SiteScope

To access SiteScope using the new interface, enter the SiteScope address in a Web browser. The default address is: http://localhost:8080/SiteScope. The first time SiteScope is deployed, there is a delay for initialization of the interface elements. SiteScope opens to the Dashboard view, as shown below.



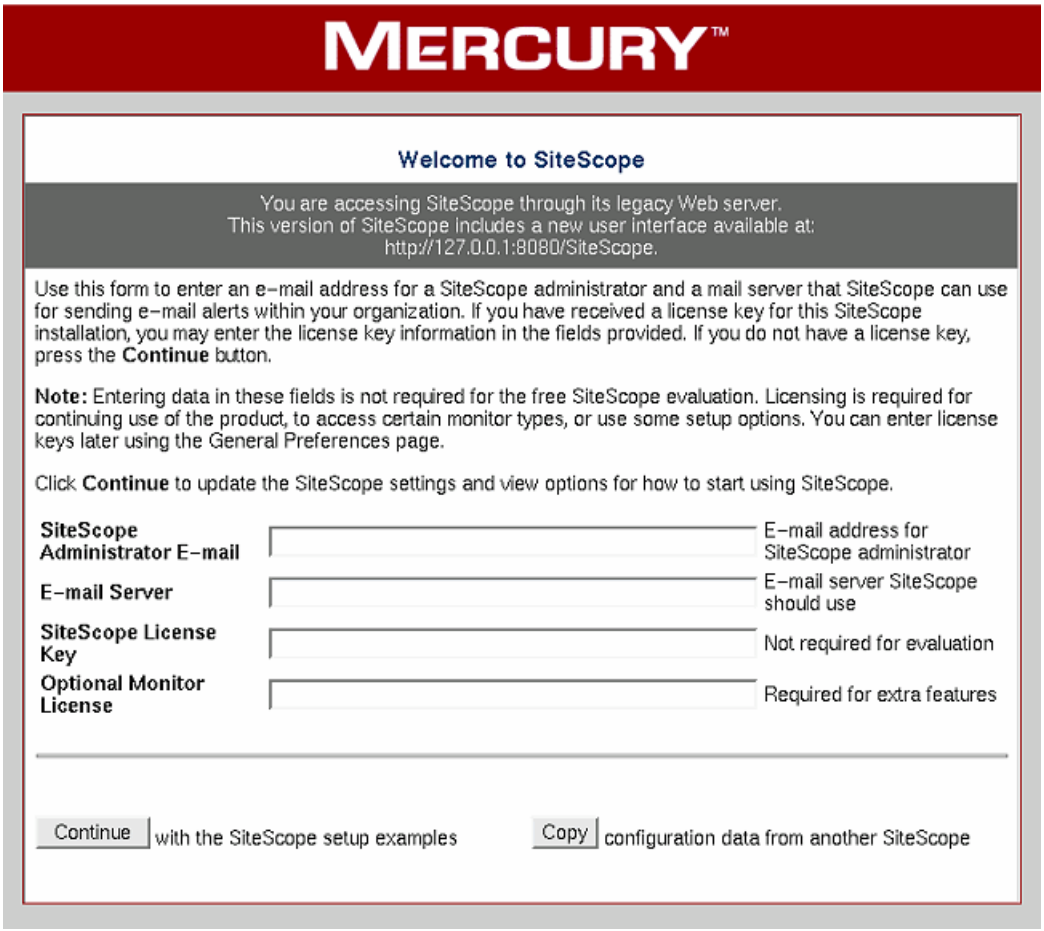
Accessing the SiteScope Classic Interface

Use the following steps to access SiteScope using the Classic interface.

To access SiteScope using the Classic interface:

1 Enter the SiteScope address in a Web browser. The default address is: http://localhost:8888/SiteScope. The first time SiteScope is deployed after installation, the SiteScope Welcome screen for first-time setup opens.

If you have upgraded or moved an existing SiteScope installation, the SiteScope main panel opens. If this is a new SiteScope installation, the SiteScope First-Time Setup screen opens.



2 Verify the SiteScope Administrator e-mail address entered during the installation process. If you did not enter an e-mail address during the installation, enter an address now. Enter the address of the SMTP mail server that SiteScope should use to forward e-mail alerts.

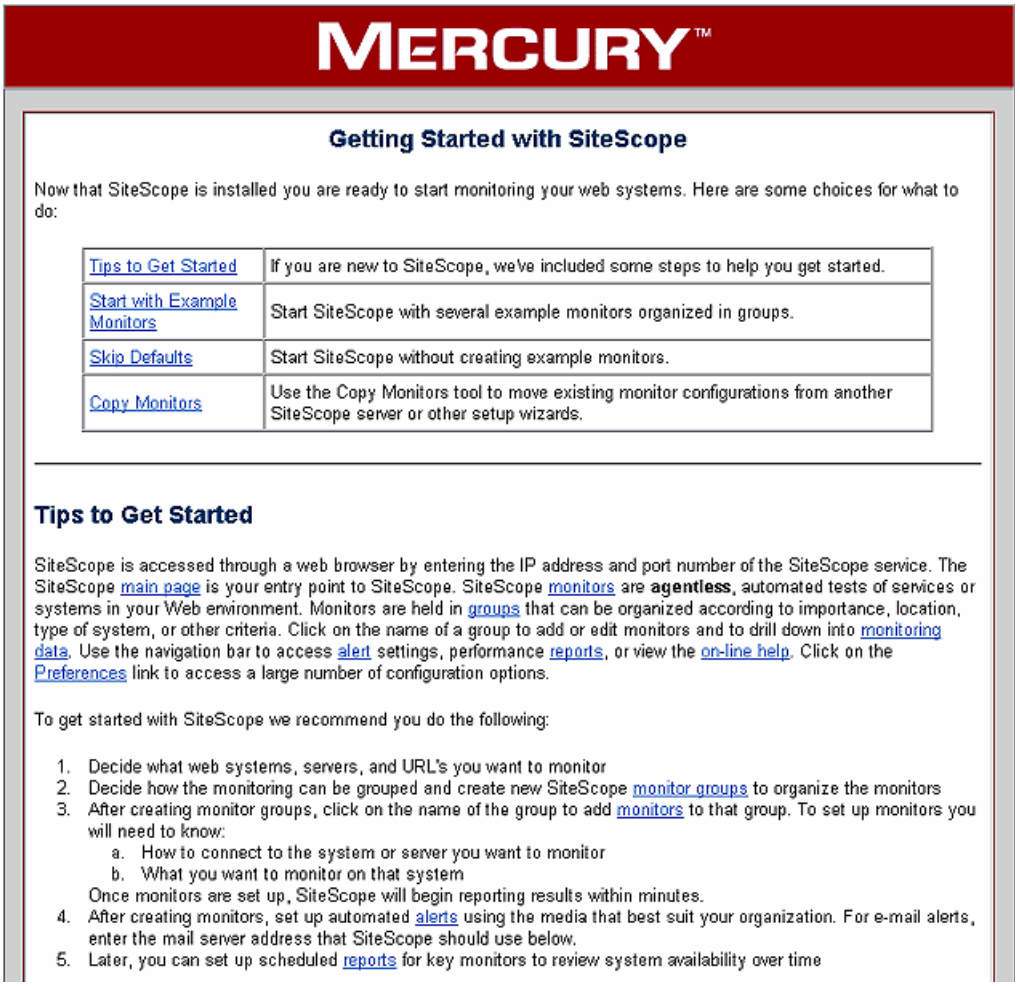
Note: SiteScope 8.0 requires a new license key. License keys from earlier versions of SiteScope are not valid to operate SiteScope 8.0. Entering an invalid license may make the product inaccessible. Contact your Mercury sales representative to convert your existing license to a SiteScope 8.0 license.

If you have received a license key or optional license for SiteScope from Mercury, you may enter the license information in the appropriate field.

Note: To use SiteScope during the free evaluation period, it is not mandatory to enter license information at this point.

If this is an installation upgrade, license information from the previous SiteScope installation is displayed. If you are changing your SiteScope license, you can enter the changes in the applicable text field.

3 Click **Continue** to continue to save any changes and proceed to the next step. An update screen opens and refreshes automatically to the SiteScope First-time Setup – Getting Started screen.



The First-time Setup - Getting Started screen presents the following options for setting up SiteScope:

- **Start Now** – This option starts SiteScope and adds a number of example monitors organized into several subgroups. These example monitors are contained within a monitor group labeled **Examples**. You can access this group by clicking on the name of the group on the SiteScope main page.
- **Skip Defaults** – This option starts SiteScope without creating any example or default monitors. The SiteScope main page is displayed without any groups. Use the **Create Group** link to add new groups as containers for SiteScope monitors.
- **Copy Monitors** – This option copies monitor and alert configurations from another SiteScope installation to this installation. This is useful when moving a SiteScope installation from one server to another.

Note: To use the **Copy Monitors** feature, the source SiteScope installation must be running and be accessible via HTTP to the target SiteScope installation.

---

4 Select the setup option you want by clicking the appropriate button. An update page opens and refreshes automatically to the SiteScope Classic main page.

At this point, the SiteScope application is ready to begin monitoring system availability in your infrastructure. If you selected to **Start Now** with the default monitor examples, you can click on the name **Examples** on the console to view the contents of the Examples group.

4

Installing SiteScope for Windows

SiteScope is designed for ease of deployment. SiteScope for Windows is available as a single, self-extracting executable file that can be downloaded from the Mercury Web site and is also available on CD-ROM. SiteScope is installed on a single server and run as a single application on the Windows platform. This means you can install SiteScope in minutes and begin monitoring your systems and servers quickly.

This chapter describes:	On page:
Installing SiteScope on Windows Platforms	41
Connecting to SiteScope on Windows Platforms	50

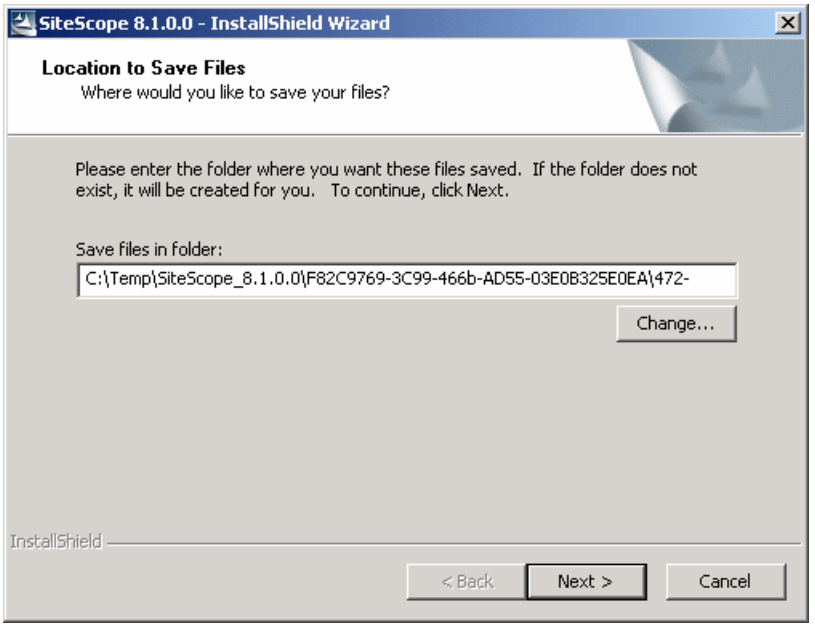
Installing SiteScope on Windows Platforms

Use the following steps to install SiteScope on Windows 2000 or 2003.

To install SiteScope on Windows platforms:

1 Download the SiteScope setup file or insert the CD-ROM containing the SiteScope software into the CD drive on the machine where you want to install SiteScope.

2 Run the SiteScope setup program. A location selection screen opens.

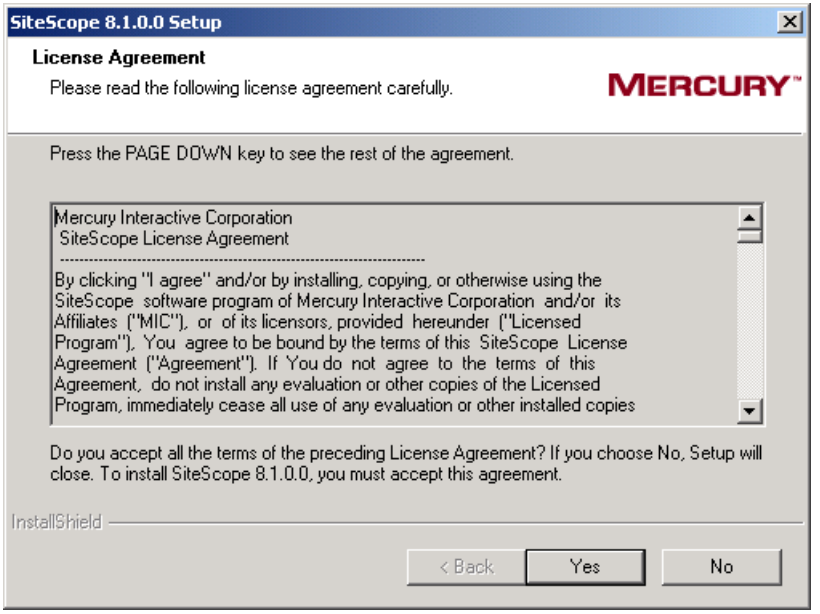


The SiteScope installation makes use of a temporary folder for extracting files used to perform the installation process.

Note: You may change the location to which the temporary files will be copied. For example, you can change the path to a more descriptive path name. You should make a note of this temporary location. After the installation is complete and SiteScope is operational, you should delete the contents of the temporary folder in order to conserve disk space.

---

3 Click **Next** to accept the default temporary folder location and continue with the installation. Alternatively, click the **Change** button to change the location for the temporary files and then click **Next** to continue with the installation. Files are automatically extracted. The License Agreement screen opens.

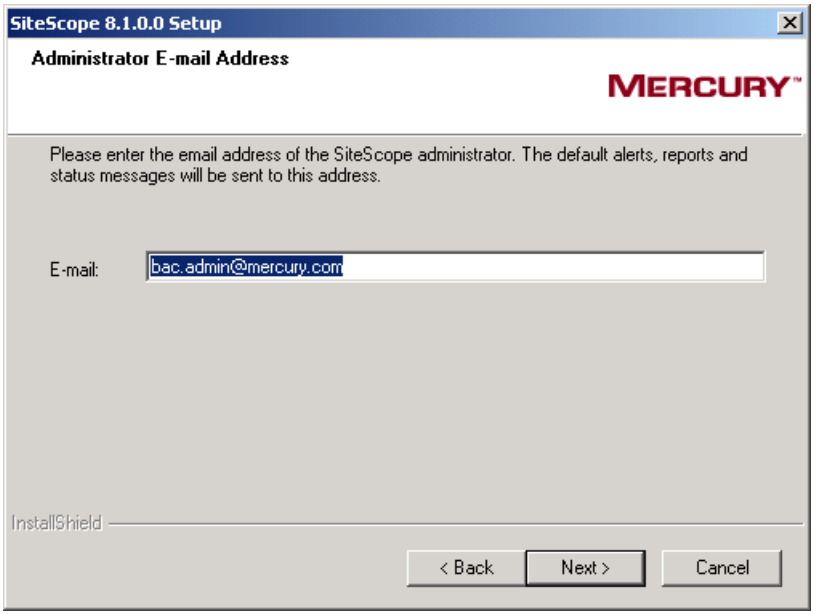


4 Read the SiteScope License Agreement.

To install SiteScope, you must accept the terms of the license agreement by clicking **Yes**. If you click **No**, the setup program will close.

After you install SiteScope, the text of the SiteScope license agreement can be found in <SiteScope root folder>\license.html.

5 Click **Yes** to confirm that you accept the Software License Agreement. The Administrator E-mail Address screen opens.

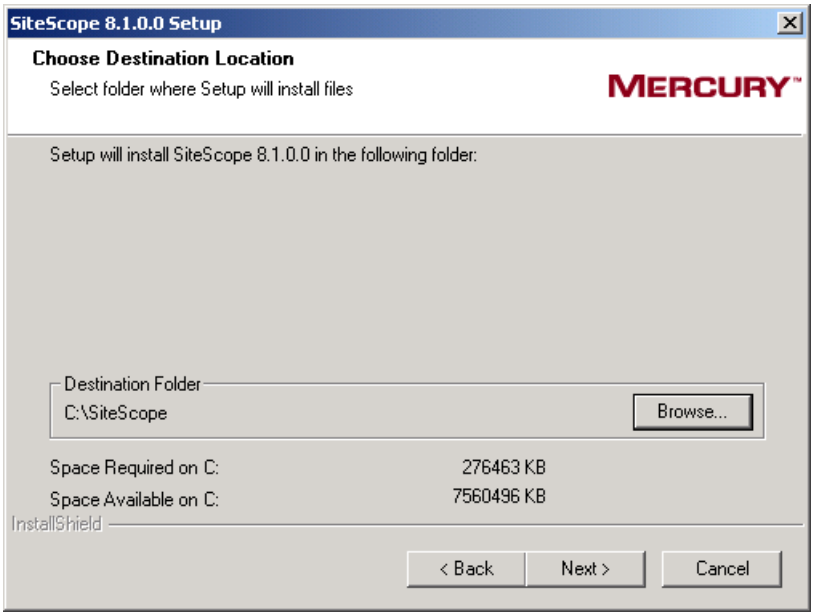


6 Enter the e-mail address that SiteScope should use to send e-mail alerts to the SiteScope administrator.

Note: You do not need to enter an e-mail address at this point to install SiteScope. You can enter this information later using the E-mail Preferences settings in SiteScope.

---

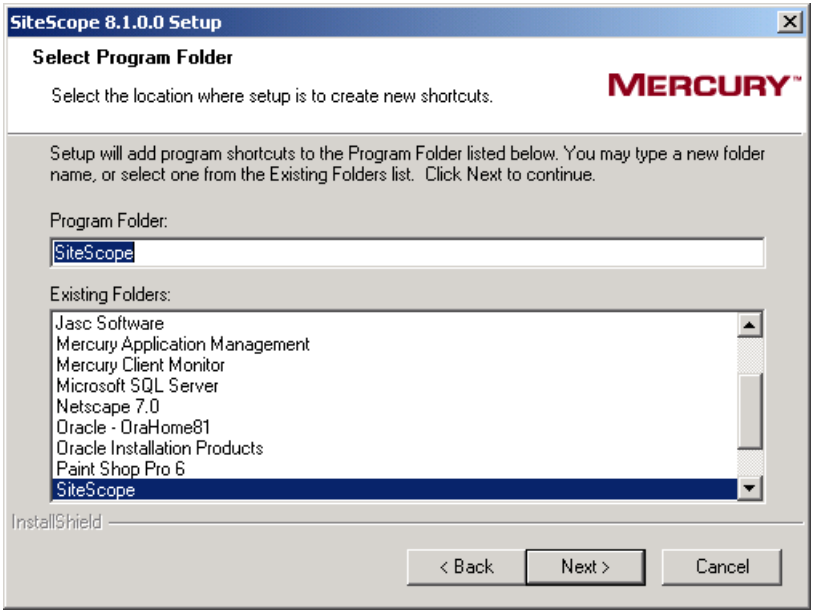
7 Click **Next** to continue. The Choose Destination Location screen opens.



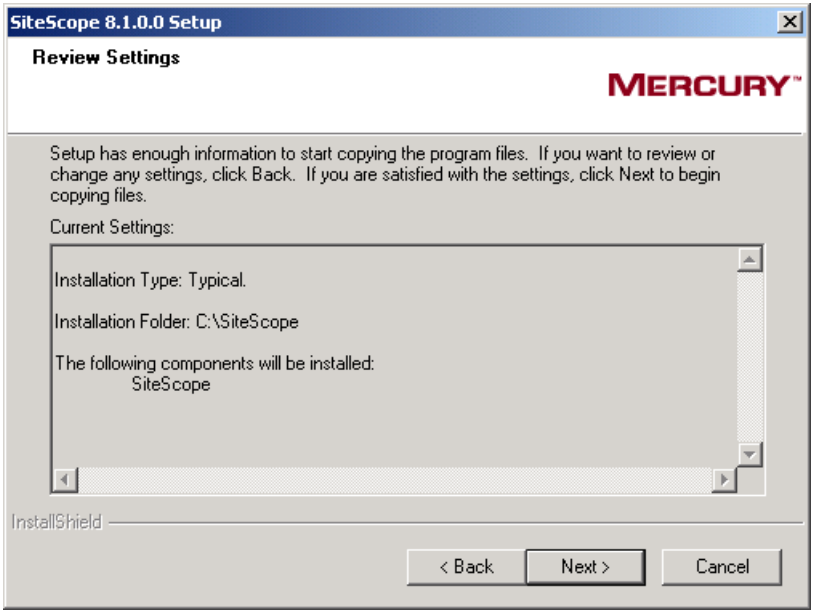
Important: Before installing SiteScope 8.1, you must have SiteScope 8.0 installed. You must install SiteScope 8.1 into the same directory as SiteScope 8.0. If you are installing SiteScope 8.0, you must create a new directory for installation of SiteScope 8.0. Do not install version 8.0 into a directory used for a previous version of SiteScope.

---

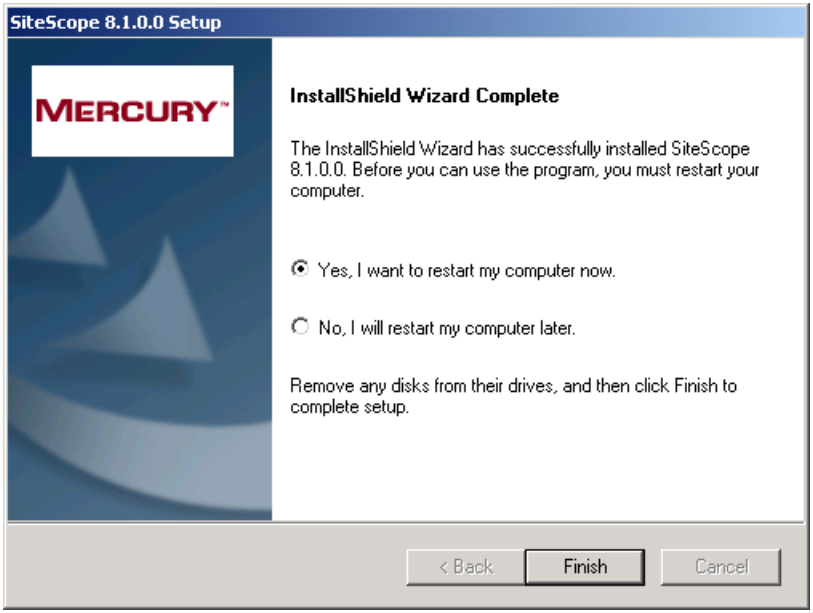
8 Select the folder where you want SiteScope to be installed. Click **Next** to accept the default installation path as shown. Click **Browse** to change the installation location. The installation path must end with a folder named SiteScope. After entering the new Destination Folder path, click **Next** to continue. The Select Program Folder screen opens.



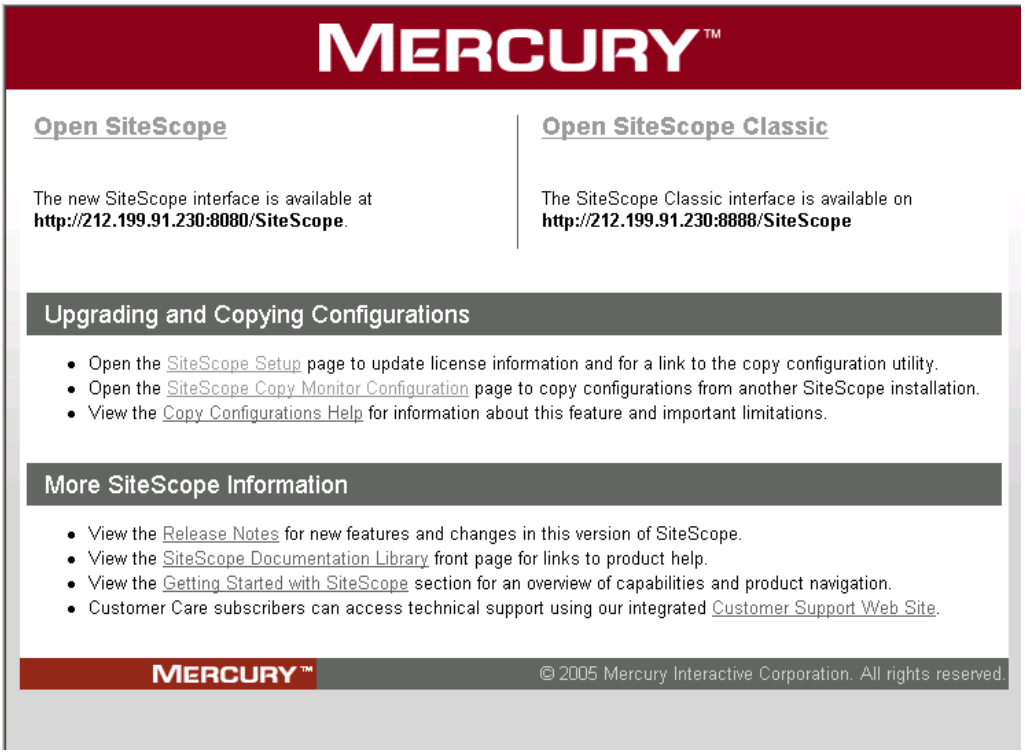
9 Select the Start Menu Program folder where you want the SiteScope program shortcuts to appear. Click **Next** to accept the default. This will create a program folder with the name SiteScope. Select an existing program folder from the selection list provided or enter a new name in the Program Folder field. Click **Next** to continue. The Review Settings screen opens.



10 Click **Next** to continue. The SiteScope installation process is started. An installation progress screen opens. When the installation process is complete, an installation completion dialogue is displayed. In many cases, you will need to restart the server where you have installed SiteScope to complete the installation.



11 Click **Finish** to complete the installation process. If the installation program determines that the server must be restarted, the restart procedure is executed. After the server is restarted and you log in, the installation wizard performs other needed setup procedures and starts the SiteScope server. The Open SiteScope page opens.



The Open SiteScope page displays the connection address for this installation of SiteScope, as well as several other links to SiteScope documentation and support information. This is a static HTML page. On Windows platforms, a shortcut to this page is added to the SiteScope program folder in the Start menu. You can use this page to access SiteScope when the application is running.

12 For the latest available functionality, download and install the latest SiteScope service pack from the same location from which you installed SiteScope.

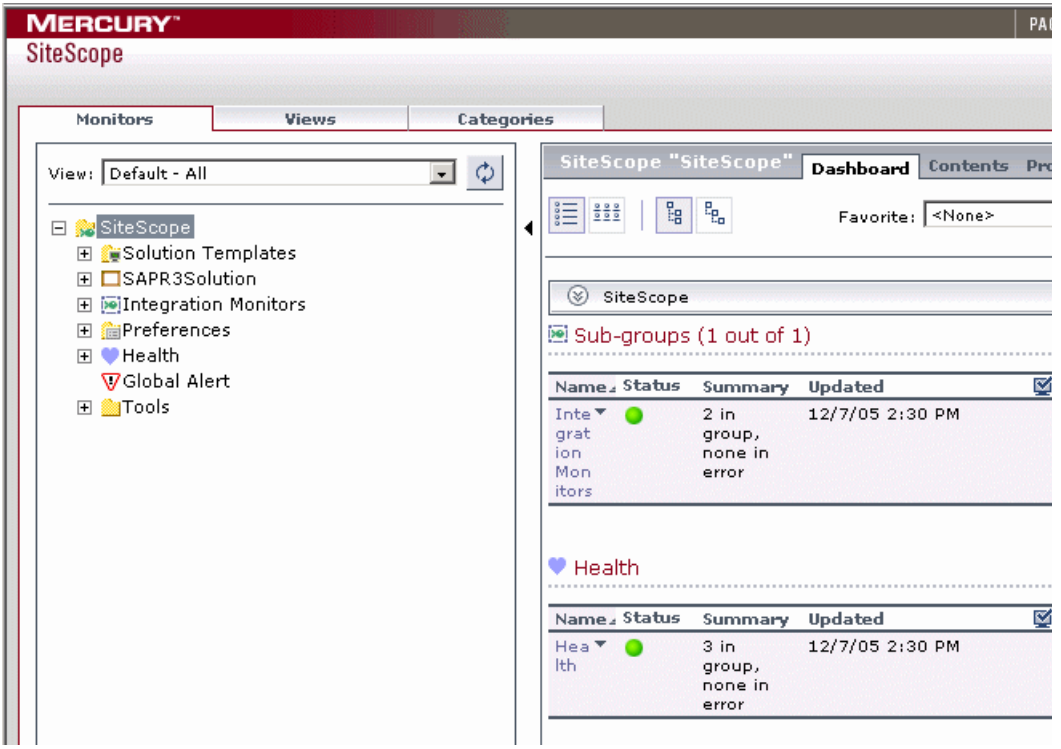
Connecting to SiteScope on Windows Platforms

SiteScope is installed to answer on two ports: 8080 and 8888. If there is another service configured to use these ports, the installation process will attempt to configure SiteScope to answer on another port. SiteScope will update the port number information in the file Open_SiteScope.htm. This file is an HTML page that is found in the SiteScope installation directory. On Windows platforms, the installation process also adds a link to this file in the **Start** > **Programs** menu for SiteScope. The Start menu folder is selected during the installation procedure.

Accessing the SiteScope 8.x Interface

To access SiteScope using the new interface, click the **Open SiteScope** link on the Open SiteScope page. A new browser instance opens. Alternatively, you can enter the address in a Web browser. The default address is: http://localhost:8080/SiteScope.

If this is the first time that this installation of SiteScope is accessed, there may be a slight delay as some of the interface elements are initialized. SiteScope opens to the Dashboard view, an example of which is shown in the following figure.



Accessing the SiteScope Classic Interface

Use the following steps to access SiteScope using the Classic interface.

To access SiteScope using the Classic interface:

1 Click the **Open SiteScope Classic** link on the Open SiteScope page. A new browser instance opens. Alternatively, you can enter the address in a Web browser. The default address is: http://localhost:8888/SiteScope. If this is the first time that this installation of SiteScope is accessed, the SiteScope Welcome screen for first-time setup opens.



2 Verify the SiteScope Administrator e-mail address entered in step 6 above. Enter the address of the SMTP mail server that SiteScope should use to forward e-mail alerts. If you have received a new license key or optional monitor license for SiteScope from Mercury, you may enter the license information in the appropriate field.

Note: SiteScope 8.0 requires a new license key. License keys from earlier versions of SiteScope are not valid to operate SiteScope 8.0. Entering an invalid license may make the product inaccessible. Contact your Mercury sales representative to convert your existing license to a SiteScope 8.0 license.

Note: It is not necessary to enter license information at this point to use SiteScope during the free evaluation period.

If you are upgrading a previous SiteScope installation, license information from the previous SiteScope installation will be displayed. If you are changing your SiteScope licensing, you can enter the changes in the applicable text field.

3 Click **Continue** to save any changes and proceed to the next step. An update screen opens and refreshes automatically to the SiteScope First-time Setup – Getting Started screen.

The First-time Setup – Getting Started screen presents several options for setting up SiteScope. The options are:

- **Start Now** - This option starts SiteScope and adds a number of example monitors organized into several subgroups. These example monitors are contained within a monitor group labeled **Examples**. You can access this group by clicking the name of the group on the SiteScope main page.
- **Skip Defaults** - This option starts SiteScope without creating any example or default monitors. The SiteScope main page is displayed without any groups. Use the Create Group link to add new groups as containers for SiteScope monitors.
- **Copy Monitors** - This option copies monitor and alert configurations from another SiteScope installation to this installation. This is useful when moving a SiteScope installation from one server to another.

Note: To use the Copy Monitors feature, the source SiteScope installation must be running and be accessible via HTTP to the target SiteScope installation.

---

4 Select the setup option you want by clicking the appropriate button. An update page opens and refreshes automatically to the SiteScope main page. The following view shows the SiteScope main page after selection of the **Start Now** setup option.

At this point, the SiteScope application is running and ready to begin monitoring system availability in your infrastructure.

If you selected to **Start Now** with the default monitor examples, you can click on the name **Examples** on the console to view the contents of the Examples group. Refer to the *SiteScope Help* for information about working with SiteScope. You click the **Help** button to access the online version of the SiteScope documentation.

5

Copying SiteScope Configurations

If you have earlier versions of SiteScope running in your environment which you want to upgrade to the current SiteScope version, you use the Copy Monitor Configuration utility to transfer existing monitor configurations. This utility provides a convenient tool for moving configuration data from one SiteScope installation to another.

The Copy Monitor Configuration utility is accessed through the SiteScope classic interface after the installation procedure is complete. It is not accessible through the new interface. For more information on how to access this utility, see "Copying Configuration Data" on page 57.

Note: Not all SiteScope configuration data is copied by the copy utility. For information on data that is not copied by this utility, see "Limitations" on page 56.

Usage

Use this utility if you are upgrading from an earlier version of SiteScope. The copy operation should be used to copy configuration data to a new SiteScope 8.0 or 8.1 installation only before any other configurations are made to the new installation. You can use this utility to copy existing SiteScope 8.0 or 8.1 configurations from one installation to another.

Note: You can manually copy configuration data files from an existing SiteScope installation to a new SiteScope 8.0 or 8.1 installation. The SiteScope installation into which you are copying configurations must not be running at the time that you paste the files into their respective directories on the new installation. This is to avoid possible configuration conflicts with the new configuration mechanism in SiteScope 8.0 or 8.1.

Requirements

The following are requirements for successfully copying SiteScope configuration data to a SiteScope 8.0 or 8.1 installation.

- You must resolve all SiteScope Health errors caused by defects in monitor group files and the **master.config** file on the SiteScope from which you want to copy configurations. These errors are detected by the MG Health and Master Health monitors respectively in SiteScope 7.9. Check the SiteScope Health group for details as necessary. If errors have been detected, be sure to make a backup copy of the files in the SiteScope\groups directory before making changes to the files to correct the errors. If you are not familiar with editing these files, contact Mercury Customer Support or Mercury Services for assistance.
- The copy operation uses HTTP requests to transfer configuration data. SiteScope includes a facility to allow configuration files to be transferred. To use this facility, the installation for the current version of SiteScope (to which configurations are copied) must to be running and accessible via HTTP (or optionally HTTPS) from the previous version of SiteScope (from which configurations are copied).

Limitations

The following are some important limitations in using the Copy Monitor Configurations utility:

- Upgrading to SiteScope 8.0 - If you are upgrading from an earlier version of SiteScope to SiteScope 8.0, the license keys are not copied. SiteScope 8.0 requires a new license key and will not operate with the license key from earlier versions of SiteScope. Contact your Mercury sales representative to obtain SiteScope 8.0 licensing to replace your existing licensing.
- Integration (EMS) Monitor Configuration Files - If you are upgrading from an earlier version of SiteScope to SiteScope 8.0, the utility does not copy the additional configuration files used by these monitor types (the files in the **SiteScope\conf\ems** directory). You must manually copy the **SiteScope\conf\ems** directory from the source machine to the target machine to exactly the same location as it was on the source machine. For example, if SiteScope 7.9.5.0 was installed in C:\SiteScope directory on one machine and 8.0 was installed in D:\SiteScope directory on another, then the ems directory should be copied to C:\SiteScope\ems on the machine where 8.0 is running. Alternatively, if the integration monitor directory remains in the new location, you must edit each integration monitor and change the **EMS Configuration File Path** to point to this new directory. If you are transferring configuration data from one SiteScope 8.0 installation to another 8.0 installation, the applicable integration monitor data is copied automatically.
- Middleware and Drivers - Middleware such as database drivers used to connect to, monitor, or log SiteScope data to external databases are not copied by the copy utility. You will need to reinstall these libraries or packages manually on the new SiteScope installation.
- Custom Monitors - Any custom monitor files are not copied by the copy utility. You will need to copy the appropriate files to the new SiteScope installation as needed.

Copying Configuration Data

You use the following steps to copy SiteScope monitor configurations from one SiteScope to another.

To copy SiteScope configurations:

1 Access the SiteScope setup page of the current version in the SiteScope Classic interface. Normally, this page will be presented when you open SiteScope using the Classic interface port number for the first time after installation and before any groups or monitors have been created. On

Windows platforms, you can click on the **Open SiteScope Classic** link on the Open SiteScope page. On all platforms, you can open the setup page URL using the following syntax:

http://<sitescope_host>:8888/SiteScope/cgi/go.exe/SiteScope?page=setup

2. On the setup page, click the **Copy** button at the bottom portion of the page. The Copy Monitor Configurations dialogue page opens.
3. Enter the host name or address of the server where the previous version of SiteScope is running in the **Remote SiteScope Server Address and Port** field. Include the port number that the source SiteScope is listening on. By default, SiteScope listens on port 8888.
4. Enter the administrator user name for the previous version of SiteScope in the **SiteScope Administrator User Name** field and the corresponding administrator password in the **SiteScope Administrator Password** field. Note that these are the user name and password configured in the User Preferences on the remote SiteScope and not the user name and password to login to the remote server through the file system. If no administrator user is defined for the source SiteScope, leave these fields blank.
5. If you want to use the HTTPS secure protocol for the data transfer, click the check box for the **Use HTTPS** item.
6. If you must use a proxy server to communicate with the source SiteScope, enter the applicable connection information in the **Proxy Server**, **Proxy Server User Name**, and **Proxy Server Password** fields.
7. If the International Version option is enabled in the source SiteScope (see the General Preferences page), click the **International Version** check box on the Copy Monitor Configuration screen.
8. Click the **Copy** button to continue. A copy confirmation screen opens.
9. Click the **Copy** button to start the copy operation. A progress display screen opens.

Note: If successful, the copy operation automatically restarts the new SiteScope installation and processes the copied configurations. You will need to make a new Web browser request for the SiteScope interface after SiteScope has restarted by entering the appropriate address and port number. For example, the new SiteScope 8.0 interface is available at http://<sitescope_host>:8080/SiteScope/. The SiteScope Classic interface is available at http://<sitescope_host>:8888/SiteScope.

6

Uninstalling SiteScope

An advantage of SiteScope's agentless architecture is the ease with which it can be uninstalled.

This chapter describes:	On page:
Uninstalling SiteScope for Windows Platforms	61
Uninstalling SiteScope for Solaris or Linux	63

Uninstalling SiteScope for Windows Platforms

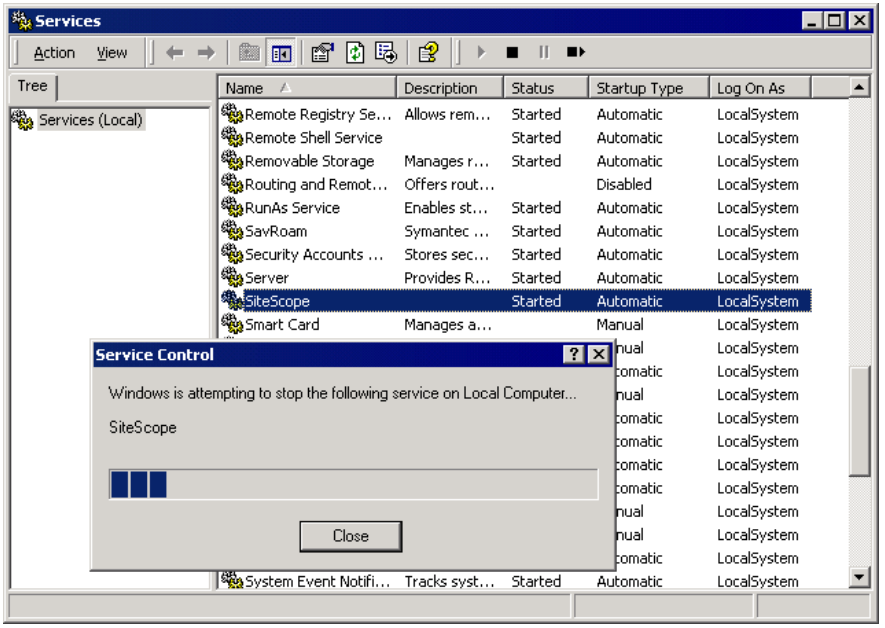
For SiteScope running on Windows platforms, the SiteScope installation includes a program to uninstall the SiteScope software from your computer.

Note: Uninstalling SiteScope does not delete the temporary setup files and archives created during the installation process. These temporary files occupy several megabytes of disk space. By default, these files are created in the C:\temp\SiteScope_8.1.0.0\ directory tree. You should delete these files manually.

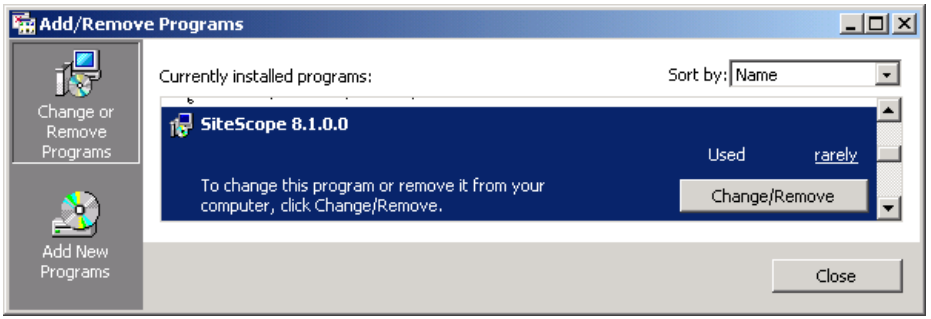
To uninstall SiteScope for Windows platforms:

1 Choose **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.

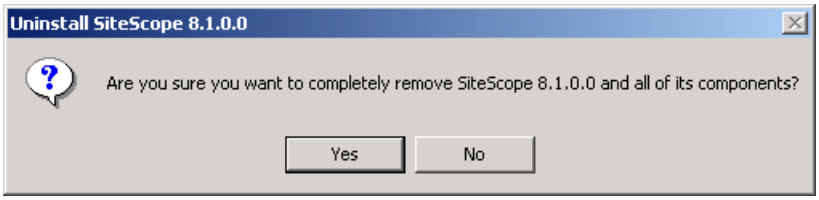
2 Select the SiteScope service in the list of services. If SiteScope is running, right-click to display the action menu and select **Stop**. Wait until the **Status** of the service indicates that it is stopped, and close the Services window.



3 Choose **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**. Select SiteScope from the list of currently installed programs.



4 Click to remove the program. A confirmation screen opens.



5 Click **Yes** to confirm the deletion of SiteScope from the server. The Remove Programs screen opens and the uninstall process starts. When the uninstall process is completed, close the Remove Programs screen.

Note: Uninstalling SiteScope does not uninstall the Java JVM or other client applications used to support SiteScope monitors. It does not delete SiteScope data log files, saved reports, or monitor configuration files. To remove SiteScope data logs, reports, and other files, you must manually delete the SiteScope installation directory and its subdirectories.

Note: Beginning with SiteScope 8.0, it is normally be necessary to restart the server to complete the uninstall process. Failure to restart the server may lead to unexpected problems for other applications.

Uninstalling SiteScope for Solaris or Linux

For SiteScope running on UNIX platforms, the SiteScope installation includes a script to uninstall the SiteScope software from your computer. If you are unable to run the script, you can delete the SiteScope files and directories manually.

Note: Uninstalling SiteScope does not delete the temporary setup files and archives created during the installation process. These temporary files occupy several megabytes of disk space. By default, these files are created in the <install_path>/SiteScopeInstall/ directory tree. You should delete these files manually.

To uninstall SiteScope for Solaris or Linux:

1. Log into the machine where SiteScope is running using the account authorized to execute scripts in the SiteScope directory. Normally this should be the account under which SiteScope is running.
2. Stop SiteScope by running the stop shell script included in the <install_path>/SiteScope directory. An example command line to run the script is:

   SiteScope/stop

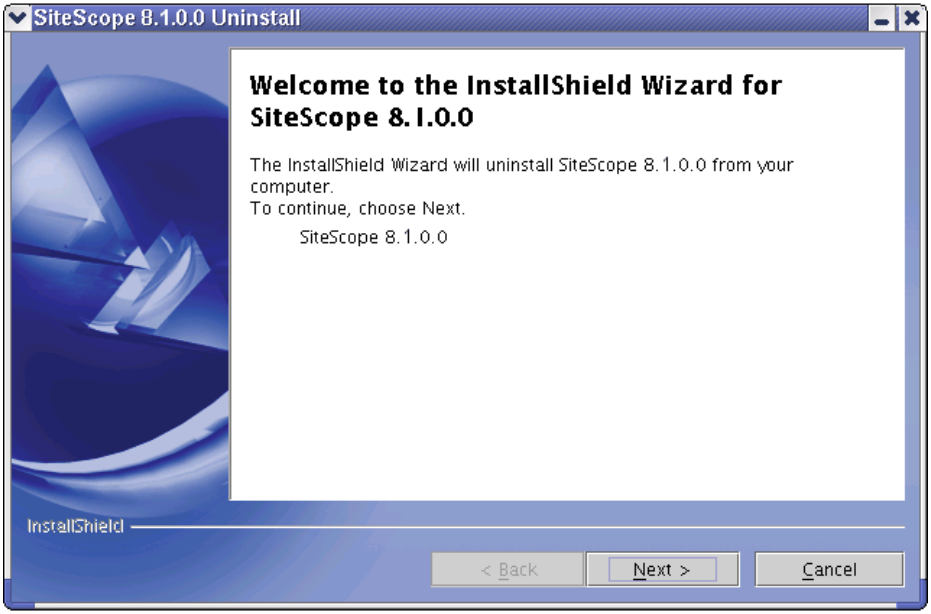
   A message is displayed indicating that SiteScope is stopped.



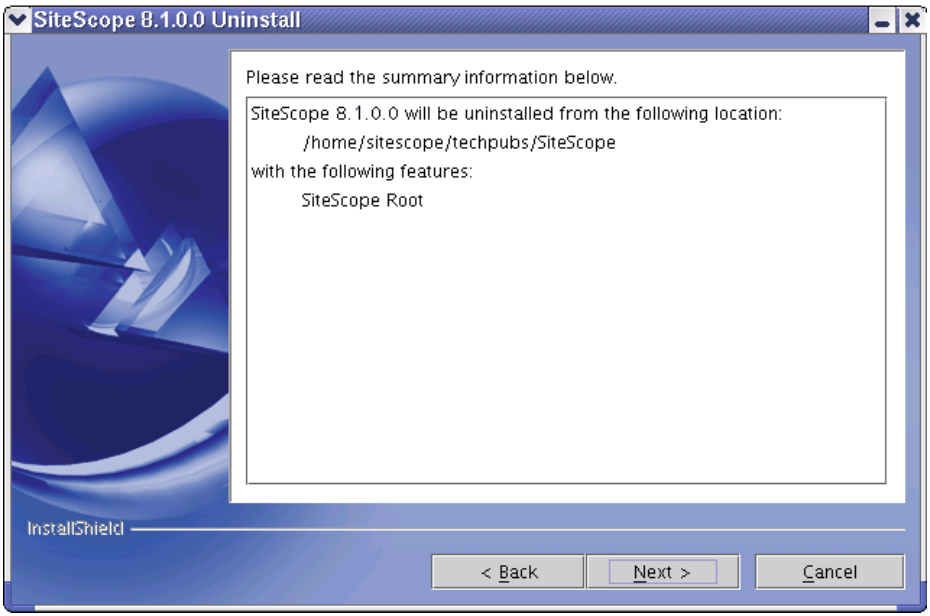
3. Run the uninstall script in the <install_path>/SiteScope/_uninst directory. An example command line to run the script is:

   SiteScope/_uninst/uninstall

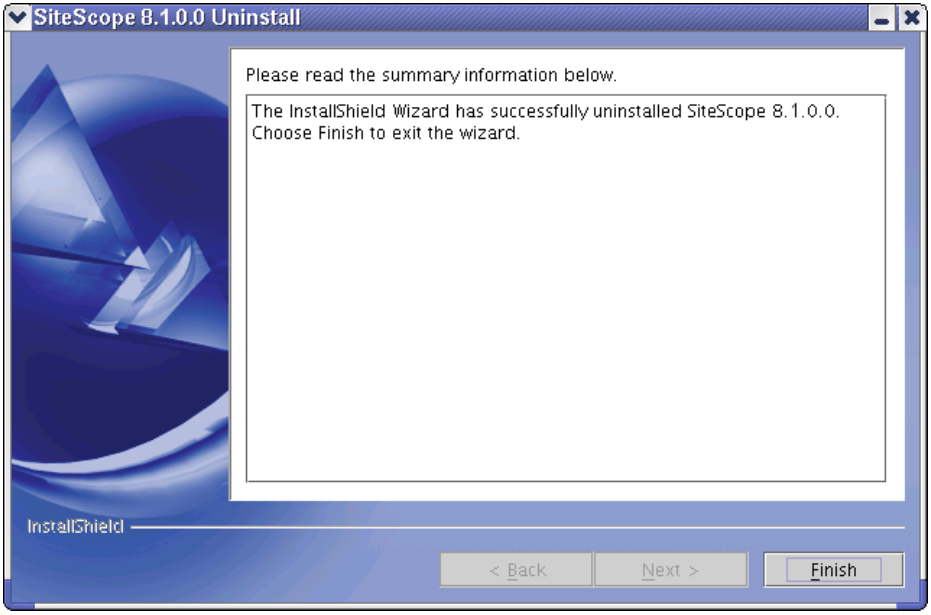
The install program is initialized and a wizard dialogue window opens.



4 Click the **Next** button to continue. A summary page opens.



5 Click the **Next** button to continue. The uninstall operation is started. Several message will be displayed in the terminal window used to run the uninstall script. A summary page opens indicating the uninstall is complete.



6 Click the **Finish** button to close the wizard and terminate the script.

Note: Running the SiteScope uninstall script does not delete all SiteScope files nor does it uninstall the Java JVM, client applications used to support some SiteScope Application monitors, or other programs.

Part II

Running SiteScope Securely

7

Hardening the SiteScope Platform

Network and system security has become increasingly important. As a system availability monitoring tool, SiteScope will necessarily have access to some system information which could be used to compromise system security if steps are not taken to secure it. This section describes several configuration and set up options that can be used to harden the SiteScope platform.

Important: In SiteScope version 8.0 and later, there are two Web servers that are active and serving two versions of the SiteScope product interface. In order to limit all access to SiteScope you must apply the applicable settings to both the SiteScope Classic Web server and the Apache Tomcat server supplied with SiteScope 8.0 and later.

Setting SiteScope User Preferences

SiteScope user profiles are used to require a username and password in order to access the SiteScope interface. After installation, SiteScope will normally be accessible to any user who has HTTP access to the server where SiteScope is running.

By default, SiteScope is installed with only one user account and this account does not have a default username or password defined for it. This is the administrator account. You should define a username and password for this account after installing and accessing the product. You can also create other user account profiles to control how other users may access the product and what actions they may perform. See the section "User Preferences" in *SiteScope Help* for more information on creating user accounts.

Restricting Access to SiteScope by IP Address

You can restrict access to SiteScope based on the IP address of the client requesting access to the application. This is a form of access control list. As noted, SiteScope 8.0 includes two product interfaces and two Web servers. The changes need to be applied to both interfaces in order to be effective.

To restrict access to the SiteScope Classic Web server, you enter the allowed IP addresses using the General Preferences settings. You must use the SiteScope Classic interface to enter these settings. This access control can be further enhanced by requiring that a username and password be used as well. See the online help for the General Preferences page in the SiteScope Classic interface for more information.

To restrict access to the SiteScope 8.0 interface using an IP access control list, you must edit the configuration file for the Tomcat server included with SiteScope. You can enable access control lists by adding a Valve component to the applicable section of the Tomcat server configuration file. See the Apache Jakarta Web site for documentation on Tomcat configuration. For example, see http://jakarta.apache.org/tomcat/tomcat-5.0-doc/config/valve.html.

Using Secure Socket Layer (SSL) to Access SiteScope

SiteScope can be configured to use SSL to control access to the product interface. Enabling this option will require that users are authenticated using a certificate. See Chapter 8, “Configuring SiteScope to Use SSL” for more information.

8

Configuring SiteScope to Use SSL

SiteScope can be configured to use Secure Sockets Layer (SSL) to restrict access to the SiteScope interface.

This chapter describes:	On page:
About Using SSL in Mercury SiteScope	73
Preparing SiteScope for Using SSL	74
Configuring SiteScope 8.0 and Later for SSL	78
Configuring SiteScope Classic for SSL	80

About Using SSL in Mercury SiteScope

You set a Mercury SiteScope server to support SSL by configuring the web server used to server the SiteScope interface to support SSL. You do this by importing a digital certificate to a key store file and then changing sever configuration settings to have SiteScope only respond to HTTPS requests.

Important: There are two web servers that are active and serving two versions of the product interface. In order to limit all access to SiteScope to HTTPS client connections, you must configure both the SiteScope Classic web server and the Tomcat server supplied with SiteScope 8.0 and later to use SSL using the steps in this section.

Preparing SiteScope for Using SSL

SiteScope is shipped with Keytool.exe. Keytool is a key and certificate management utility. It enables users to administer their own public/private key pairs and associated certificates for authentication using digital signatures. It also allows users to cache the public keys of other persons and organizations they communicate with. This is installed in <SiteScope install path>/SiteScope/java/bin directory.

Important: The process for creating, requesting, and installing a digital certificate requires close attention to detail. Be sure to make a note of the parameters and command line arguments that you use in each step of the process as it is very important that you use the same values though out the procedure.

You can find out more about Keytool at the Sun Microsystems Web site:

http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html

Using a Certificate from a Certificate Authority

You can use a digital certificate issued by a Certificate Authority. In order to use this option, you need a digital certificate that can be imported into the key storage file used by Keytool. If your organization does not currently have a digital certificate for this purpose, you will need to make a request to a Certificate Authority to issue you a certificate.

You use the following steps to create a KeyStore file and a digital certificate request.

To create a certificate request file for a Certificate Authority:

1 Remove the serverKeystore file that is located in the SiteScope\groups directory. You can delete it or simply move it to a different directory.

Note: This file must be removed before performing the following steps.

---

2 Create a key pair. To do this you need to run the command line listed below from the SiteScope\java\bin directory. The values in italics are variables that you provide with information specific to your organization

---

Note: Note: This command and all others you use must be entered on a single line. The line is divided here to fit on this page.

```
keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment,
O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -
alias yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -
storepass passphrase -keyalg "RSA" -validity valdays
```

This command will create a file called "serverKeystore" in the SiteScope\groups directory. SiteScope will use this KeyStore file to store the certificates used in your secure sessions. Make sure you keep a backup copy of this file in another location.

Note: The value of a -dname option must be in the following order where the italicized values are replaced by values of your choosing. The keywords are abbreviations for the following:

CN = commonName - Common name of a person (for example, "Warren Pease")
OU = organizationUnit - Small organizational unit (for example, "NetAdmin")
O = organizationName - Large organization name (for example, "ACMe-Systems, Inc.")
L = localityName - Locality (city) name (for example, "Palo Alto")
S = stateName - State or province name (for example, "California")
C = country - Two-letter country code (for example, "US")

Note: The subcomponents within the -dname (distinguished name string) variable are case-insensitive and they are order-sensitive, although you do not have to include all of the subcomponents. The -dname variable should represent your company and the CN is the domain name of the Web server on which SiteScope is installed.

Note: The value of -storepass is a password used to protect the KeyStore file. This password must be at least 6 characters long. You will need to use this password to import to and remove certificate data from the KeyStore file.

Note: The -alias variable is an alias or nickname you use to identify an entry in your KeyStore.

After you receive your certificate from a Certificate Authority (the reply message should include a file called cert.cer), you need to import this certificate into the KeyStore file you created using the steps above. The file should be called serverKeystore. You use the following steps to import the certificate for use with SiteScope.

To import a certificate from a Certificate Authority:

1. Import the certificate data into the KeyStore file by running the following command from the SiteScope\java\bin directory:

   keytool -import -trustcacerts -alias yourAlias -file cert.cer -keystore ..\..\groups\serverKeystore

2. To change SiteScope to use a secured connection, you need to add or modify certain settings or configuration files in SiteScope. See the sections "Configuring SiteScope 8.0 and Later for SSL" on page 78 or "Configuring SiteScope Classic for SSL" on page 80 depending on the product interface you will be using.

Using a Self-Signed Certificate

Alternatively, you can generate a self signed certificate for use with SiteScope. To do this, you use the -selfcert option to have the Keytool utility generate a self-signed certificate using the following steps.

To use a self-signed certificate:

1 Remove the serverKeystore file that is located in the SiteScope\groups directory. You can delete it or simply move it to a different directory.

Note: This file must be removed before performing the steps listed below.

---

2 Run the following command from the SiteScope\java\bin directory. The values in italics are variables that you fill in with information specific to your organization.

Note: This command and all others you use must be entered on a single line. The line is divided here to fit on this page.

```
keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment,
O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -
alias yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -
storepass passphrase -keyalg "RSA" -validity valdays
```

3 Run the following command, also from the SiteScope\java\bin directory:

```
keytool -selfcert -alias yourAlias -sigalg "MD5withRSA" -keypass password -
dname "CN=www.yourDomain.com, OU=yourDepartment,
O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -
keystore ..\..\groups\serverKeystore
```

4 To change SiteScope to use a secured connection, you need to add or modify certain settings or configuration files in SiteScope. See the sections "Configuring SiteScope 8.0 and Later for SSL" on page 78 or "Configuring SiteScope Classic for SSL" on page 80 depending on the product interface you will be using.

Configuring SiteScope 8.0 and Later for SSL

In order to enable SSL on Tomcat you need to make changes to the configuration files used by the Tomcat server.

1. Find the file SiteScope\Tomcat\conf\server.xml.
2. Locate the section of the configuration file that looks like the following:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
-->
```

3 Change this section to the following:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="<SiteScope_install_path>\SiteScope\groups\serverKeystore"
keystorePass="testing"
/>
```

Where <SiteScope_install_path> is the path to your SiteScope installation.

By default Tomcat looks for a .keystore file in the SiteScope user's home directory. Using the serverKeystore should allow user's to use the same cert for both the old SiteScope interface and the new SiteScope interface if they choose. If not then they can just specify the location to the cert they want to use for Tomcat.

For more information on enabling SSL for the Tomcat server see: http://jakarta.apache.org/tomcat/tomcat-5.0-doc/ssl-howto.html

After enabling Tomcat to use SSL using this example, the new SiteScope interface will be available at a URL with the following syntax:

https://<sitescopeserver>:8443/sitescope

Configuring SiteScope Classic for SSL

To change SiteScope to use a secured connection, you need to add or modify the several settings in the master.config file.

To configure SiteScope Classic to use SSL:

1. Using a text editor, open the file: <SiteScope_install_path>\SiteScope\groups\master.config.
2. In this file, locate or add the following parameter:

   _httpSecurePort=

3. Select a port number to be used for SSL connections to SiteScope. The number you use for the _httpSecurePort parameter can be set to any available port number. It is recommended that you use a port number other than 8888, which is the default port for accessing SiteScope using HTTP (unsecured). Add this port number to be the value of the _httpSecurePort setting.
4. Locate or add the following parameters, adding the applicable passphrase and keypass words:

   _httpSecureKeyPassword=passphrase
   _httpSecureKeystorePassword=keypass

   In order to access SiteScope using HTTPS exclusively, you will need to modify the following parameters in the master.config file to disable access via HTTP as shown below, substituting the applicable values for those items in italics.:

   _httpPort=
   _httpSecurePort=portnumber
   _httpSecureKeyPassword=passphrase
   _httpSecureKeystorePassword=keypass

Note: All the parameters in the master.config file are case and syntax sensitive. Be sure not to add any extra spaces or lines to the file.

---

5 Save the changes to the master.config file.

6 Stop and restart the SiteScope service for the changes to become effective.

You should now be able to access SiteScope using HTTP for example, for access from inside the firewall, at the default address of:

http://server_IP_address:8888

You should also be able to access SiteScope using HTTPS at the following address, based on steps in the example above:

https://server_IP_address:8899

Part III

External Integrations and Functionality

9

Integration with Mercury Business Availability Center

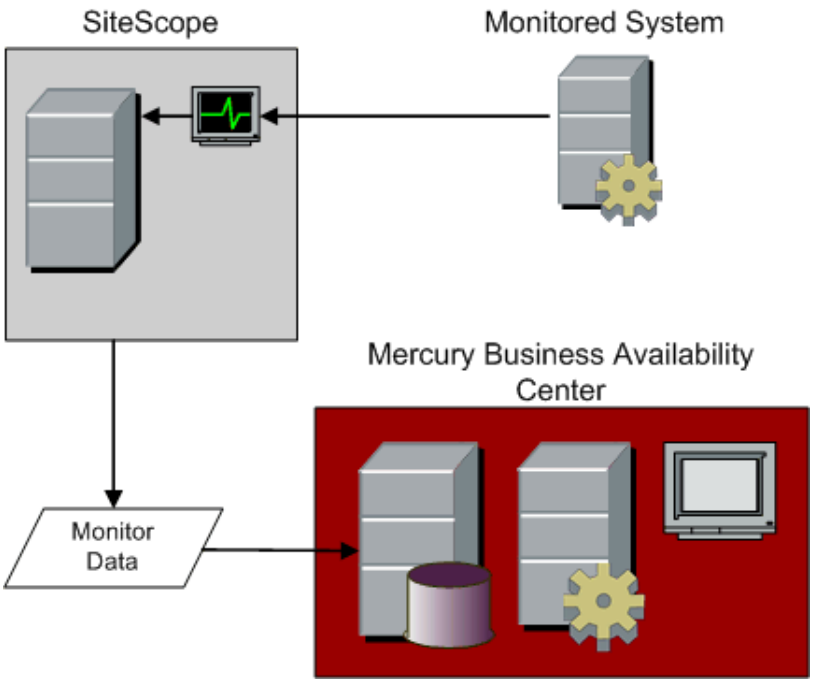
SiteScope can be configured to be a data collector reporting to Mercury Business Availability Center. You can use this to integrate SiteScope's system level availability monitoring data with the performance monitoring and analysis capabilities of Mercury Business Availability Center. SiteScope also includes features for monitoring the availability of Mercury Business Availability Center servers known as the Mercury Self-Alert Monitor.

This chapter describes:	On page:
Understanding SiteScope Integration with Mercury Business Availability Center Products	86
Registering SiteScope to Mercury Business Availability Center	90
Changing the Core Server to Which SiteScope Sends Data	95
Setting Up the Mercury Self-Alert Monitor Group	99
Using SSL for SiteScope-Mercury Business Availability Center Communication	99
Reporting Status per Measurement	101
Troubleshooting Data Reporting to Mercury Business Availability Center	102

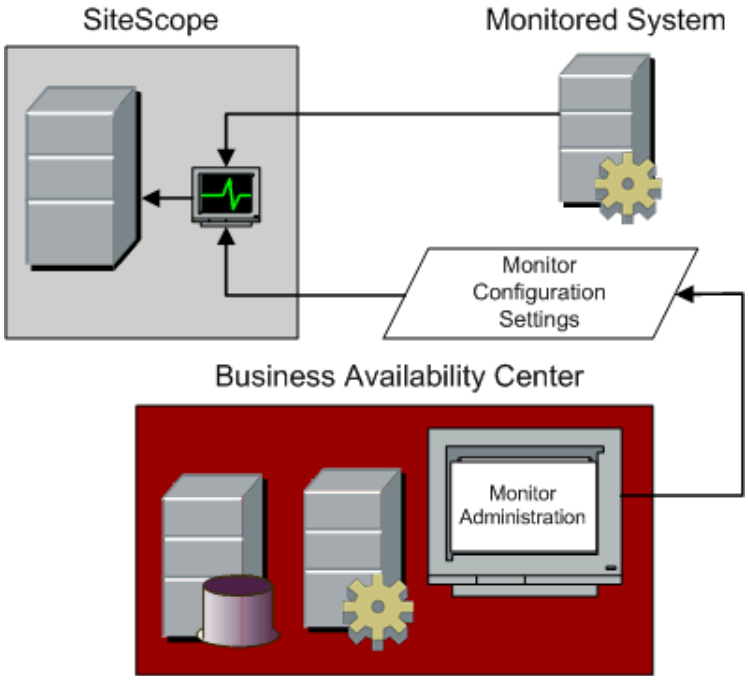
Understanding SiteScope Integration with Mercury Business Availability Center Products

SiteScope, as a standalone application, is an agentless solution for system availability monitoring. SiteScope can be used as a data collection agent for Mercury Business Availability Center. Mercury Business Availability Center use one or more data collectors to collect data about end-users, business processes, and systems.

When registered as an agent to a Mercury Business Availability Center, the data and measurements collected by SiteScope monitors can be passed on to the Mercury Business Availability Center database for use in reports and analysis. Monitor data can be sent for all monitors or for selected monitors. The following diagram illustrates the use of SiteScope as a data collection agent for Mercury Business Availability Center.



Mercury Business Availability Center includes a Monitor Administration console. This feature allows you to manage SiteScope monitor configurations for one or more SiteScope servers through a central console. This level of SiteScope integration is separate from the integration of SiteScope monitor data with Mercury Business Availability Center. The following diagram illustrates the use of the Monitor Administration console in Mercury Business Availability Center to manage SiteScope monitor configurations. See the Mercury Business Availability Center Documentation Library for more information.



Version Support Matrix

There are two main aspects of compatibility between SiteScope and Mercury Business Availability Center. The first is data logging which is the process of logging data collected by SiteScope to Mercury Business Availability Center for the purposes of real-time status, reporting, Service Level Management, and so forth. The second aspect of compatibility is Monitor Administration which refers to configuring SiteScope (including deploying monitors) from within Mercury Business Availability Center. The following table contains compatibility information regarding these two aspects and the various combinations of SiteScope and Topaz/Mercury Business Availability Center releases.

- 1 = Data logging support
- 2 = Monitor Administration support
- X = Not supported

SiteScope Version	Mercury Business Availability Center Version				
	6.1	6.0	5.1	5.0	Topaz 4.5SP1-4.5SP3
SiteScope 8.1.2 (recommended version for 6.1)	1,2	1,2	1,2	1	1
SiteScope 8.1, 8.1.1	1,2	1,2	1,2	1	1
SiteScope 8.0 SP2	1,2	1,2	1,2	1	1
SiteScope 8.0, 8.0 SP1	1	1	1,2	1	1
SiteScope 7.9.5.x	1,2	1,2	1,2	1	1
SiteScope 7.9.1.0	1	1	1	1,2	1
SiteScope 7.9.0.0	1	1	1	1	1
SiteScope 7.8.1.0, 7.8.1.2	X	X	1	1	1

When SiteScope is registered as a data collector reporting data to Mercury Business Availability Center, it may also be accessed as a standalone product, if the SiteScope installation has not been attached to Mercury Business Availability Center Monitor Administration. This section describes how to register SiteScope as a data collector for Mercury Business Availability Center. For details on attaching a SiteScope to Monitor Administration, see "Managing SiteScope in the Monitor Tree" in *Managing SiteScope*.

Note: Due to product changes and corresponding product name changes, these products may be referred to as Topaz, Mercury Application Management, or Mercury Business Availability Center.

Note: You must access SiteScope through the SiteScope Classic interface to access the Mercury Business Availability Center Server Registration form. An example URL syntax for the form is:
http://sitescopeserver:8888/SiteScope/cgi/go.exe/SiteScope?page=topazPrefs&account=administrator
This form is found under the **Preferences** -> **Mercury BAC** link in the SiteScope Classic interface.

Accessing Mercury Self-Alert Monitor

At the bottom of the Mercury Business Availability Center Server Registration page is the Mercury Self-Alert Monitor Settings section. This section is used to configure the SiteScope server to serve as a Mercury Self-Alert Monitor. The set up is automated to configure the necessary monitors for the applicable Mercury Business Availability Center deployment. See "Mercury Self-Alert Monitor" on page 115 for more information about this functionality.

Registering SiteScope to Mercury Business Availability Center

To enable logging of SiteScope monitor data to Mercury Business Availability Center server, you need to configure SiteScope as an agent reporting to Mercury Business Availability Center. You use the Mercury Business Availability Center Server Registration form to register the SiteScope server as an agent reporting to a Mercury Business Availability Center server.

Note: You can also register SiteScope as an agent reporting to Mercury Business Availability Center by using the Monitor Administration console in Business Availability Center.

The registration process involves three steps:

1 Creating an empty SiteScope profile in Mercury Business Availability Center. An empty profile means a new profile which will be defined in the Monitor Administration console.

Note: Specifying an empty profile will not import the SiteScope configuration data.

---

2 Specifying connection parameters for SiteScope to connect to the Mercury Business Availability Center server.

Note: If the Topaz Admin Server/Mercury Business Availability Center Core Server to which you are connecting is on a different machine than the Topaz Graph Server/Mercury Business Availability Center Core Server that SiteScope is to report to, you need to provide connection information for both servers under the Optional Settings section. This is applicable for Topaz 4.5 and earlier.

---

3 Selecting the Mercury Business Availability Center profile in which you want to save SiteScope data.

Note: Monitors created in SiteScope before registration to Mercury Business Availability Center have their Mercury Business Availability Center Logging option set to not report to Mercury Business Availability Center. After you configure SiteScope as an agent reporting to Mercury Business Availability Center, the default state for new monitors created in SiteScope is to log their monitoring data to Mercury Business Availability Center. To change Mercury Business Availability Center Logging options use either the Mercury Business Availability Center Logging settings on the Manage Monitors/Groups page or edit a specific monitor and check the Stop Logging to Mercury Business Availability Center check box in the Add/Edit monitor screen. See the Manage Monitors and Groups page for more information about enabling and disabling logging to Mercury Business Availability Center.

The following describes the sections and options on the Mercury Business Availability Center Server Registration page.

Step 1 - Creating an empty SiteScope profile in Mercury Business Availability Center.

See the section "SiteScope Profile Integration Status" for the steps you use to create a SiteScope profile.

Step 2 - Specifying Connection Parameters to Mercury Business Availability Center Servers

Complete the form as indicated below, and then click the Register button to complete the action.

After registration you may control SiteScope logging to Mercury Business Availability Center with the following buttons:

Update Mercury Business Availability Center Settings

Change any of the Required or Optional settings.

Disable/Enable

Stop SiteScope from logging to Mercury Business Availability Center. This state can be toggled at any time.

Re-Synchronize

Force SiteScope to resend all its configuration data. This data consists of all the Group and Monitor definitions.

Reset

This will delete all Mercury Business Availability Center related settings.

Note: Mercury Business Availability Center will not allow the selection of a previously used SiteScope profile.

Edit Core Server

Used to change the Mercury Business Availability Center Core Server to which SiteScope reports data. This is only applicable in environments where more than one Core servers are deployed.

Required Settings

The following are the required settings for registering SiteScope with Mercury Business Availability Center.

Business Availability Center machine name/IP address

Enter the name or IP address of the Mercury Business Availability Center server machine to which you want this SiteScope to connect. Enter the server name if the Mercury Business Availability Center to which you are registering this SiteScope is installed on a single machine or server. If the Mercury Business Availability Center to which you are registering this SiteScope is deployed in a distributed installation on more than one server, enter the name of the Core Server for the BAC deployment.

SiteScope agent machine location

Enter the location of the SiteScope server or agent that you are connecting to Mercury Business Availability Center. You can specify any value that helps you identify the location of this specific SiteScope server.

Business Availability Center user name

Enter the user name of a Mercury Business Availability Center administrator-level user.

Business Availability Center user password

Enter the password for the user specified above.

Optional Settings

The following optional settings may be required in some environments.

Business Availability Center Server

The following are security options for the Business Availability Center Web server.

Authentication username and Authentication password

If the Mercury Business Availability Center server is configured to use basic authentication, specify the username and password required to access the server in the text fields provided.

Use SSL (HTTPS protocol)

Check this box if the Mercury Business Availability Center server is configured to use the HTTPS protocol.

Business Availability Center Agent Server

Set these values only if the Mercury Business Availability Center Core Server is installed on a different machine than the Mercury Business Availability Center Centers Server. This is applicable for Topaz version 4.5 and earlier.

Server name/IP address

Enter the name of the Topaz Agent Server/Mercury Business Availability Center Core Server to which you want this SiteScope to connect.

Authentication username and Authentication password

If the Topaz Agent Server/Mercury Business Availability Center Core Server is configured to use basic authentication, specify the username and password required to access the server.

Use SSL (HTTPS protocol)

Check this box if the Topaz Agent Server/Mercury Business Availability Center Core Server is configured to use the HTTPS protocol.

Proxy Server

Set these values only if access to Mercury Business Availability Center requires the use of a proxy server.

Proxy Address

If applicable, enter the proxy server address.

Proxy Username

Enter the username for the proxy server.

Proxy Password

Enter the password for the specified user.

Step 3 - Selecting the Mercury Business Availability Center Profile

After you have specified the connection properties and SiteScope has successfully connected to the Mercury Business Availability Center server, you must associate your SiteScope server with a profile. Select the SiteScope profile in which Mercury Business Availability Center will store the data collected by SiteScope (the SiteScope profile must have been previously defined in the Topaz Admin Center/Mercury Business Availability Center Monitor Administration console). Then click the Submit button.

Notes:

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

Changing the Core Server to Which SiteScope Sends Data

Beginning in SiteScope 8.0.0.1, you can change the Core Server to which a SiteScope agent reports its data. Generally, this is only applicable if you are working with a Mercury Business Availability Center deployment with components installed on more than one server.

Note: You must use the SiteScope Classic interface to make this change.

Limitations

The following are limitations for using this feature:

- This feature is only available for SiteScope 8.0.0.1 and above. To change the Core Server for earlier versions of SiteScope you must execute command line procedures on the SiteScope server. The details of the procedures vary according to the version of SiteScope you are using.
- This feature can only be used for changing the Core Server for a SiteScope that is already registered with a given Mercury Business Availability Center installation. It cannot be used to add a new SiteScope, or to connect a SiteScope to a different Mercury Business Availability Center system.

Changing the Core Server to Which SiteScope Sends Data (Version 8.0.0.1 and Later)

To change the Core Server to which SiteScope sends data:

1. Access the SiteScope Classic interface. You do this by opening a Web browser to the SiteScope server address. By default, the address will have the form of http://<SiteScope server>:8888.
2. Click the **Preferences** button on the SiteScope main navigation bar. The General Preferences page opens.
3. Select the **Mercury BAC** link from the Preferences submenu. The Mercury Business Availability Center Server Registration page opens.
4. Click the **Edit Core Server** button
5. In the Business Availability Center server machine name/IP address box, enter the required Core Server name or IP address
6. Click **Update** to save the changes.
7. Restart SiteScope

Changing Core Server for Other SiteScope Versions

Prior to the 8.0.0.1 version of SiteScope, changing the Core Server to which a SiteScope reports its data requires that you execute a command line procedure on the SiteScope server. As part of each procedure, you specify a name of a file which is created during the process and used to modify SiteScope configuration information. The following describe the steps you use for earlier versions of SiteScope.

To change the Core Server to which SiteScope 7.8.1.2 or 7.8.1.0 sends data:

1. Make a note of the name of the currently configured Core Server to which the SiteScope is sending its data. Also note the name of the other Core Server to which you want to redirect the SiteScope reporting.
2. Access the server where the subject SiteScope is running.
3. Open a command line window on the SiteScope server and change the working directory to the <SiteScope_install_path>\SiteScope\classes directory.

4 Execute the following command line to export the relevant SiteScope configuration data to a text file. Substitute a valid filename for the <filename> parameter (for example, sitescope2bca.txt):

..\java\bin\java -cp COM.freshtech.TopazIntegration.TopazServerSettings export *<filename>*

5 Open the exported text file with a text editor. Replace all occurrences of the original Core Server name with the name of the new Core Server.

6 Save the changes to the text file.

7 Stop the SiteScope service.

8 In the command line window, execute the following command line to import the relevant SiteScope configuration data to SiteScope. Substitute the name of the text file for the <filename> parameter as indicated:

..\java\bin\java -cp COM.freshtech.TopazIntegration.TopazServerSettings import <filename>

9 Restart the SiteScope service.

To change the Core Server to which SiteScope 7.9.1.0 or 7.9.5 sends data:

1 Make a note of the name of the currently configured Core Server to which the SiteScope is sending its data. Also note the name of the other Core Server to which you want to redirect the SiteScope reporting.

2 Access the server where the subject SiteScope is running.

3 Open a command line window on the SiteScope server and change the working directory to the <SiteScope_install_path>\SiteScope\classes directory.

4 Execute the following command line to export the relevant SiteScope configuration data to a text file. Substitute a valid filename for the <filename> parameter (for example, sitescope2bca.txt):

..\java\bin\java -cp COM.freshtech.TopazIntegration.AMSettingsManager export *<filename>*

5 Open the exported text file with a text editor. Replace all occurrences of the original Core Server name with the name of the new Core Server.

6 Save the changes to the text file.

7 Stop the SiteScope service.

8 In the command line window, execute the following command line to import the relevant SiteScope configuration data to SiteScope. Substitute the name of the text file for the <filename> parameter as indicated:

..\java\bin\java -cp COM.freshtech.TopazIntegration.AMSettingsManager import <filename>

9 Restart the SiteScope service.

To change the Core Server to which SiteScope 8.0.0.0 sends data:

1 Make a note of the name of the currently configured Core Server to which the SiteScope is sending its data. Also note the name of the other Core Server to which you want to redirect the SiteScope reporting.

2 Access the server where the subject SiteScope is running.

3 Open a command line window on the SiteScope server and change the working directory to the <SiteScope_install_path>\SiteScope\classes directory.

4 Execute the following command line to export the relevant SiteScope configuration data to a text file. Substitute a valid filename for the <filename> parameter (for example, sitescope2bca.txt):

..\..\java\bin\java.exe -Dtopaz.home=..\..\conf\ems\tools -classpath ..\..\WEB-INF\classes;..\..\WEB-INF\lib\jgl.jar;..\..\WEB-INF\lib\xdr.jar;..\..\WEB-INF\lib\tmc_ex_data.jar;..\..\WEB-INF\lib\xdr_utils.jar;..\..\WEB-INF\lib\jms.jar; COM.freshtech.TopazIntegration.AMSettingsManager export *<filename>*

5 Open the exported text file with a text editor. Replace all occurrences of the original Core Server name with the name of the new Core Server.

6 Save the changes to the text file.

7 Stop the SiteScope service.

8 In the command line window, execute the following command line to import the relevant SiteScope configuration data to SiteScope. Substitute the name of the text file for the <filename> parameter as indicated:

..\..\java\bin\java.exe -Dtopaz.home=..\..\conf\ems\tools -classpath ..\..\WEB-INF\classes;..\..\WEB-INF\lib\jgl.jar;..\..\WEB-INF\lib\xdr.jar;..\..\WEB-INF\lib\tmc_ex_data.jar;..\..\WEB-INF\lib\xdr_utils.jar;..\..\WEB-INF\lib\jms.jar; COM.freshtech.TopazIntegration.AMSettingsManager import *<filename>*

9 Restart the SiteScope service.

Setting Up the Mercury Self-Alert Monitor Group

You must register SiteScope with Mercury Business Availability Center for the Mercury Self-Alert Monitor group to work correctly. You can subsequently disable the connection, if you do not want SiteScope to report to Mercury Business Availability Center.

To set up the Mercury Self-Alert Monitor group:

1. Select the Enable Mercury Self-Alert Monitor check box.
2. SiteScope displays a link to the Mercury Self-Alert Monitor Settings page. Click this link, edit the Self-Alert Monitor Settings on the next page, and click Save Settings.
3. For the rest of the procedure to set up Mercury Self-Alert Monitor, see "Mercury Self-Alert Monitor" on page 115.

   You click the **Edit Mercury Self-Alert Monitor Settings** link to make changes to an existing Mercury Self-Alert Monitor set up. See "Mercury Self-Alert Monitor" on page 115 for more information.

Using SSL for SiteScope-Mercury Business Availability Center Communication

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

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

---

Note: You only need to specify these settings for the case that the certificate installed on the Mercury Business Availability Center machine is not signed by a root Certificate Authority (CA). For example, if you are using a certificate signed by a Certificate Authority like Verisign, you do not need to change these settings.

You can import the self-signed certificate into the same keystore file used for other SiteScope monitors but that is not required. You can create a separate keystore for the Mercury Business Availability Center server certificate.

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

1. Obtain a copy of the self-signed certificate from the Mercury Business Availability Center server saved in a DER-encoded binary X.509 format. Normally, the certificate file has an extension of .cer.
2. Import the into a keystore on the SiteScope server using the procedures described in Accessing SiteScope via HTTPS.

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

---

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

   _sslTrustedCertKeyStoreFile=<path>\<filename>

   _sslTrustedCertKeyStorePassword=<keystorepassword>

   _sslAcceptAllUntrustedCerts=<boolean>

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

   _sslTrustedCertKeyStoreFile=c:\keystores\topaz.keystore

   _sslTrustedCertKeyStorePassword=sUp3rS3cr3tP@ssw0RD

   _sslAcceptAllUntrustedCerts=false

4 Save the changes to the file.

5 Restart the SiteScope server.

Reporting Status per Measurement

By default, SiteScope reports status to Mercury Business Availability Center based on the status of the monitor. When measurements are included in Mercury Business Availability Center reporting, the monitor passes its status to the monitor's individual measurements. The monitor's status is calculated based on worst child. This means that the status for all the measurements in a monitor are calculated based on the monitor's worst child and not the status of the measurement itself. Also, if a measurement does not have its own status, it is reported to have the monitor's status.

You can now configure SiteScope to report the status for each measurement based on the individual measurement's status and not based only on the monitor's status. This enables Mercury Business Availability Center to more accurately report status for the monitor and its measurements.

To configure reporting monitor status per measurement:

1 Open the **master.config** file found in the **<SiteScope root directory>\groups** directory.

2 Change the value of the **_enableQualityPerMetric** property to true. (By default, this value is false which means that status is reported per monitor.)

Troubleshooting Data Reporting to Mercury Business Availability Center

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

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

Note: By default, the threshold number of data files is set to 1,000 files. This setting is configurable in the master.config file by modifying the _topazMaxPersistenceDirSize property.

After the connection between SiteScope and the Mercury Business Availability Center server is restored, you must manually copy the files from these folders to the <SiteScope_root>\cache\persistent\topaz\data folder. It is recommended that you only copy these files when the data folder is empty to avoid overloading the system with large amounts of data to upload. When the number of data.old folders exceeds a specified threshold, by default 10 folders, the oldest folders will be deleted.

Note: The number of data.old folders to keep is configurable in the master.config file by modifying the _topazMaxOldDirs property.

10

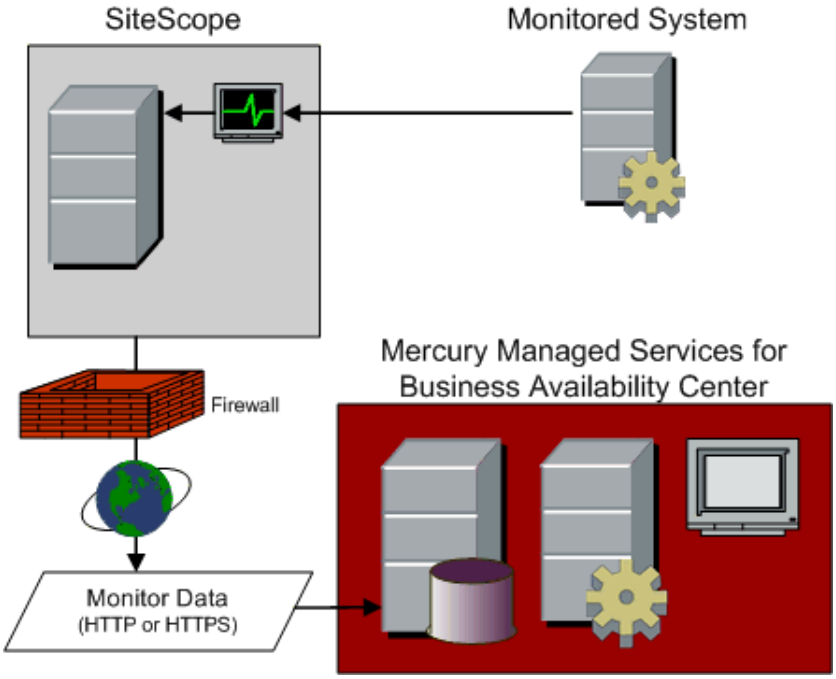
Integrating SiteScope with Mercury Managed Services

SiteScope can be configured to be an agent reporting to Mercury Business Availability Center. You can use this to integrate SiteScope's system level availability monitoring data with the performance monitoring and analysis capabilities of Mercury Managed Services for Mercury Business Availability Center.

This chapter describes:	On page:
Understanding SiteScope Integration with Mercury Managed Services.	104
Registering SiteScope to Mercury Managed Services	105

Understanding SiteScope Integration with Mercury Managed Services.

SiteScope, as a standalone application, is an agentless solution for system availability monitoring. SiteScope can be used as a data collection agent for Mercury Managed Services for Mercury Business Availability Center. This service can use one or more agents to collect data about end-users, business processes, and systems. The following diagram illustrates the use of SiteScope as a data collection agent for Mercury Managed Services.



When registered as an agent to Mercury Managed Services, the data and measurements collected by SiteScope monitors can be passed on to the Managed Services database for use in reports and analysis. Monitor data can be sent for all monitors or for selected monitors.

Registering SiteScope to Mercury Managed Services

Registering SiteScope as a remote data collection agent for Mercury Managed Services involves three steps:

1 Creating an empty SiteScope profile in Mercury Managed Services service account. An empty profile means a new profile which will be defined in the Monitor Administration console.

Note: Specifying an empty profile will not import the SiteScope configuration data.

---

2 Specifying Connection Parameters to Mercury Managed Services Servers

3 Selecting the Mercury Managed Services Profile

When SiteScope is registered as a data collection agent reporting data to a Mercury Managed Services, it may continue to be accessed as a standalone product.

Note: You must access SiteScope through the SiteScope Classic interface in order to access the Mercury Managed Services Registration form. An example URL syntax for the form is:
http://sitescopeserver:8888/SiteScope/cgi/go.exe/SiteScope?page=topazPrefs&account=administrator&topazMS=true
This form is found under the **Preferences** -> **MMS** link in the SiteScope Classic interface.

Step 1 - Creating a SiteScope Profile in Mercury Managed Services

See the section “SiteScope Profile Integration Status” for the steps you use to create a SiteScope profile in a Mercury Managed Services service account.

Step 2 - Specifying Connection Parameters to Mercury Managed Services Servers

You use the Mercury Managed Services Server Registration form to configure SiteScope to be an agent reporting to Mercury Managed Services for Business Availability Center. Complete the form as indicated below, and then click the **Register** button to connect to the server.

Required Settings

Complete the settings in the Required Settings section as follows:

SiteScope agent machine location

Enter the location of the SiteScope server or agent that you are connecting to Mercury Business Availability Center Managed Services. You can specify any value that helps you identify the location of this specific SiteScope server.

Business Availability Center Managed Services user name

Enter the user name of a Mercury Managed Services administrator-level user.

Business Availability Center Managed Services user password

Enter the password for the user specified above.

Optional Settings

The Optional Settings section includes configuration options that may be necessary in certain environments.

Proxy Server

Set these values only if access to Mercury Managed Services requires the use of a proxy server.

Address

If applicable, enter the proxy server address.

Username

Enter the username for the proxy server.

Password

Enter the password for the specified user.

Step 3 - Selecting the Mercury Managed Services Profile

After you have specified the connection properties and SiteScope has successfully connected to the Managed Services server, you must associate your SiteScope server with a MMS profile. Select the MMS profile in which Mercury Managed Services will store the data collected by SiteScope (the profile must have been previously defined in the Mercury Managed Services service account). Then click the Submit button.

Note:

- Only profiles not in use by any other SiteScope or Mercury Managed Services agent appear in the list.
- When viewing reports in Mercury Managed Services, you select this profile to see the SiteScope data.
- It is recommended that you use the word “SiteScope” in the profile name to more easily identify SiteScope profiles in the Mercury Managed Services Web site.

11

Integrating SiteScope with Mercury SiteSeer

SiteScope can be integrated with a Mercury SiteSeer Hosted Service account. In this way you can view system availability data from inside and outside the firewall in a single interface.

This chapter describes:	On page:
Understanding Integration with Mercury SiteSeer	110
Settings for SiteSeer Integration	111

Note: Beginning with SiteScope 8.0, SiteSeer integration into SiteScope is available only in the SiteScope Classic interface. This feature is not supported in the new SiteScope interface.

Understanding Integration with Mercury SiteSeer

Mercury SiteSeer is a remote service for monitoring system availability from outside the firewall. SiteSeer is built on SiteScope technology. This makes the data collected by SiteSeer directly compatible with SiteScope data.

You have the monitoring information from your SiteSeer remote monitoring account displayed as a group on the SiteScope main panel. When you click on the SiteSeer group name the SiteSeer account screen opens. You use the Back button in your browser to return to the SiteScope panel.

Note: Only one SiteSeer account may be added to a SiteScope installation.

You use the SiteSeer Preferences form to specify the SiteSeer connection and login information and test the connectivity with the SiteSeer service. Before you can do this you must have a current SiteSeer account. The SiteScope server you want to integrate with SiteSeer must also have HTTP or HTTPS access to the SiteSeer Hosted Service server where you account is running.

Note: You must access SiteScope through the SiteScope Classic interface in order to access the SiteSeer Preferences form and to view SiteSeer data. An example URL syntax for the SiteSeer Preferences form is:
http://sitescopeserver:8888/SiteScope/cgi/go.exe/SiteScope?page=siteseerPrefs&account=administrator
This form is found under the **Preferences** -> **SiteSeer** link in the SiteScope Classic interface.

Settings for SiteSeer Integration

The SiteSeer Preferences form is divided into two sections: Required Settings and Advanced Options. This section describes the settings in these two sections and how you use them to configure SiteScope to communicate with a SiteSeer account.

Required Settings

The Required Settings section includes the information that SiteScope needs to connect to a remote SiteSeer service account.

SiteSeer Account

Enter the name of your SiteSeer account. The account name is normally the domain name specified in your e-mail address. You can determine what it is by looking at the URL for your SiteSeer account. For example, if your SiteSeer URL is:

http://siteseer.mercuryinteractive.com/SiteScope?account=mycompany.com

then your account name is mycompany.com

SiteSeer Username

Enter the user name used to login to your SiteSeer account. This will be the same username as is displayed on the main screen of your SiteSeer account.

SiteSeer Password

Enter the password used to login to the SiteSeer account.

SiteSeer Host Name

Enter the host name of the SiteSeer service. This is usually siteseer2.mercuryinteractive.com or siteseer.mercuryinteractive.com. Look at the URL for your SiteSeer account to determine if yours is different. For example, if your URL is:

http://siteseer2.mercuryinteractive.com/SiteScope?account=mydot.com

your host name is siteseer2.mercuryinteractive.com.

Advanced Options

The advanced options section lets you further control access and display of your SiteSeer account information in the SiteScope interface. Complete the items as applicable and click the Save Changes button.

Disabled

Checking this box will hide the SiteSeer group on the SiteScope main panel display. This does not disable any monitors currently active on the subject SiteSeer account.

SiteSeer Title

Enter an optional title that you want to use to label the SiteSeer account group in the SiteScope panel. By default, SiteSeer is used as the group name.

SiteSeer Proxy

If you are required to use a proxy server in order to access your SiteSeer account, enter the proxy address or domain name here.

SiteSeer Proxy Username

If you are using a proxy, enter your proxy username.

SiteSeer Proxy Password

If you are using a proxy, enter your proxy password here.

Hide SiteSeer Group

Check this option to hide the display of the SiteSeer group in the SiteScope panel

Automatic SiteSeer Login

Check this box to allow automatic login to the SiteSeer account.

SiteSeer Read Only Username

Enter the username used to log in to your SiteSeer account for read only access. This is used if you have defined a SiteSeer login account other than the default administrator account. This would normally be the "user" account.

SiteSeer Read Only Password

Enter the password used to log in to your SiteSeer account for read only access.

12

Mercury Self-Alert Monitor

Mercury Self-Alert Monitor is a tool you use to monitor the Mercury Business Availability Center environment to verify that it is functioning correctly and to help troubleshoot possible problems.

This chapter describes:	On page:
Understanding the Mercury Self-Alert Monitor Group	115
Working with the Mercury Self-Alert Monitor Group	117
Mercury Self-Alert Monitor Templates	122
Mercury Self-Alert Monitor Troubleshooting	125
Troubleshooting Directory and Log File Errors	126

Understanding the Mercury Self-Alert Monitor Group

Mercury Self-Alert Monitor is a SiteScope monitor group that monitors the machines on which you have deployed Mercury Business Availability Center servers and components. It includes both system level monitoring of services, processes, server resources, the CMDB and end-to-end monitoring of the last reported data time from Business Process Monitor or Client Monitor data collectors.

When you enable the Mercury Self-Alert Monitor, SiteScope automatically creates a group containing monitors for Mercury Business Availability Center services and components registered with the applicable Mercury Business Availability Center installation. Each monitor checks a key component of the Mercury Application Management service.

The components that are monitored by the Self-Alert Monitor include:

- Core Server
- Centers Server
- Data Processing Server
- Client Monitor
- Database Server
- Business Process Monitor
- SiteScope

The Self-Alert monitors are configured using monitor templates. The templates include the conditions under which a warning or error status is reported. The status of a monitor is calculated according to default rules in the monitor templates. The monitors are set up to report when a component is no longer available or reduced performance is detected. You can customize the status threshold rules by editing the Self-Alert monitors.

Note: The Mercury Self-Alert Monitor can be configured and managed using only the SiteScope Classic interface.

Note: The SiteScope machine on which the Mercury Self-Alert Monitor group is run must use the same system time zone setting as the machine where the Mercury Business Availability Center management database is run.

The Mercury Self-Alert Monitor creates and uses many of the standard SiteScope monitors and two SiteScope monitor types unique to the Self-Alert group: the Host Last Connection Time Monitor and the Host Last Reported Data Time Monitor. For details, see "Host Last Connection Time Monitor" on page 135, and "Host Last Reported Data Time Monitor" on page 141.

You can disable and enable monitors, for example, when you know in advance that monitors will be in error, such as during routine maintenance.

Note: The templates used to create the Self-Alert monitors do not automatically create alert definitions. You must create alert definitions and associate them with the monitors or groups in the Self-Alert Monitor group to receive automated alerts. The Mercury Self-Alert Monitor group can use all SiteScope alert methods, such as Script alerts and SNMP trap alerts. For details, see "Introducing SiteScope Alerts" in *Configuring SiteScope Alerts*.

Working with the Mercury Self-Alert Monitor Group

The following is an overview of the steps you use to setup and work with the Mercury Self-Alert Monitor group:

1 Set up the Mercury Self-Alert Monitor group.

You set up the Mercury Self-Alert Monitor group to monitor Mercury Business Availability Center machines using the SiteScope classic interface. For details, see "Setting Up the Mercury Self-Alert Monitor Group" on page 118.

2 Set up a baseline for the Mercury Self-Alert Monitor group.

To ensure that the Self-Alert Monitor group works reliably, you must set up a baseline for Mercury Business Availability Center. You use the baseline to compare subsequent behavior and performance. For details, see "Creating a Baseline for the Mercury Self-Alert Monitor Group" on page 122.

3 Set up SiteScope alerts for the Mercury Self-Alert Monitor group.

For effective system management, set up alert definitions for the Mercury Self-Alert Monitor group to send automated alerts to administrators when problems are detected. For details, see "Introducing SiteScope Alerts" in *Configuring SiteScope Alerts*.

4 View current monitor status.

You can see the current status of Self-Alert monitoring by viewing the Self-Alert monitor group. The worst reported status is displayed as the status icon for the group. You view individual monitor status by opening the Monitor

Group Detail page for the group or subgroup that contains the applicable monitor.

5 Set up SiteScope reports for the Mercury Self-Alert Monitor group.

You can run Quick reports to view the recent history of the Mercury Self-Alert monitors. You can also set up scheduled reports for these monitors that will show the performance of the Mercury Business Availability Center services over a regular time interval. For details, see "SiteScope Quick Report" in *Configuring SiteScope Reports*.

This section includes the following topics:

➤ "Setting Up the Mercury Self-Alert Monitor Group" on page 118

➤ "Managing the Mercury Self-Alert Monitor Group" on page 120

Setting Up the Mercury Self-Alert Monitor Group

You set up Mercury Self-Alert Monitor as a monitor group using the SiteScope Classic interface. During the set up process you choose which services the Self-Alert Monitor group should monitor. SiteScope automatically retrieves information about the applicable Mercury Business Availability Center components.

To set up the Mercury Self-Alert Monitor group:

1 In the SiteScope Classic interface, click **Preferences** > **Mercury BAC**. The Mercury Business Availability Center Server Registration page opens.

2 If SiteScope is configured to report to Mercury Business Availability Center, the **Required Settings** boxes are filled in. Skip to step 5 below. If SiteScope is not configured to report to Mercury Business Availability Center, fill out the **Required Settings** fields as indicated. Click the **Register** button.

Note: It is recommended to register SiteScope to report to Mercury Business Availability Center for the Self-Alert Monitor group to work correctly. If you do not want SiteScope to report other data to Mercury Business Availability Center, you can subsequently disable the connection.

---

3 In the next page, select a profile name. Click **Save Profile**. You are returned to the main page. Continue to step 4.

   If you do not want SiteScope to report to Mercury Business Availability Center, you do not have to select a profile. Click the browser back button to return to the Mercury Business Availability Center Server Registration page. Skip the next step and continue at the step below.

4 Choose **Preferences** > **Mercury BAC** using the SiteScope navigation menus to return to the Mercury Business Availability Center Server Registration page.

5 Scroll to the bottom of the page to the section entitled **Mercury Self-Alert Monitor Required Settings**. Click **Configure Monitors**.

   SiteScope displays a message that there is nothing to monitor (because you have not yet selected the services to monitor).

6 Click **Edit Mercury Self-Alert Monitor Settings**.

7 In the Mercury Self-Alert Monitor Settings page, select the Mercury Business Availability Center services that you want the Mercury Self-Alert Monitor group to monitor.

8 Click **Save Settings**. The Mercury Self-Alert Monitor Configuration Result page displays the results of SiteScope's attempt to create subgroups for the Mercury Business Availability Center components.

   Results are displayed in red or black: black signifies that SiteScope was able to create a group for a Mercury Business Availability Center machine; red signifies that SiteScope created a group on a machine that requires administrative privileges for remote access (the components that are monitored on that machine appear in bold).

   If all groups are displayed in black, you can continue with the set up. If any group is displayed as red, you must configure remote server access for that server. See the steps in the section below.

   SiteScope displays the Mercury Business Availability Center Machine View that shows the name, location, and Mercury Business Availability Center service for each machine.

9 Click the **SiteScope** button in the navigation menu to return to the SiteScope main view.

The new Mercury Self-Alert Monitor group is displayed in the SiteScope main view. You click on the group name to open the group detail page and view status of individual monitors and subgroups.

You must configure remote access for any machines that are displayed in red. After you configure the remote server settings, you reconfigure the machine in the Mercury Self-Alert Monitor Settings page using the following steps.

To reconfigure Self-Alert Monitor:

1. In the SiteScope Classic interface, click **Preferences** > **Mercury BAC** to open to the Mercury Business Availability Center Server Registration page.
2. In the Mercury Business Availability Center Machine View table, clear the check box of the machine whose components you want to reconfigure.
3. Click **Save Settings**.
4. In the Self-Alert Monitor Configuration Result page, click **Edit Mercury Self-Alert Monitor Settings**.
5. In the Mercury Business Availability Center Machine View table, select the check box of the machine whose components you want to reconfigure.
6. Click **Save Settings**.

Managing the Mercury Self-Alert Monitor Group

You can make various modifications and updates to the Mercury Self-Alert Monitor Group once you have set up the group.

Disabling the Mercury Self-Alert Monitor Group

You can disable the Mercury Self-Alert Monitor group, and prevent the group from appearing in the SiteScope Preferences pages.

To disable the Mercury Self-Alert Monitor group:

1. Locate the file **master.config**, in the **<SiteScope root directory>\groups** folder.

Note: Before making any changes to this file, back up the original file to a safe location.

---

2 Open the **master.config** file using a plain text editor.

3 Find the key _disableTopazWatchdog= and set the value to true.

4 Save the changes to the file.

5 Stop and restart the SiteScope service.

Updating the Mercury Self-Alert Monitor Path

If the Mercury Business Availability Center you want to monitor is installed on a volume other than volume C of the remote server, you must change the path of the Mercury Business Availability Center folder in the Mercury Self-Alert Monitor configuration file on the SiteScope machine. You use the following steps to update the path to the folder.

To update the Mercury Business Availability Center path:

1 Open the **watchdog.config** file in the <**SiteScope root directory**>**groups** folder.

2 Locate the row with the pattern _twdTopazFolder=C$\Mercury Application Management.

3 Change the letter C in the value string to the be the volume drive letter on which Mercury Business Availability Center is installed.

4 If the Mercury Business Availability Center installation folder is shared, write the name by which it is shared. For example, if the Mercury Business Availability Center installation folder is shared by the name AppManagement, replace C$\MercuryAM with AppManagement.

5 Save the changes to the configuration file.

6 Stop and restart the SiteScope service.

Reconfiguring a Mercury Self-Alert Monitor Component

You can reconfigure a specific Mercury Self-Alert Monitor component.

To reconfigure a Mercury Self-Alert Monitor component:

1. In the SiteScope Classic interface, click **Preferences** > **Mercury BAC** to open the Mercury Business Availability Center Server Registration page.
2. In the Mercury Business Availability Center Machine View table, clear the check box of the machine whose monitors you want to reconfigure.
3. Click **Save Settings**.
4. In the Self-Alert Monitor Configuration Result page, click **Edit Mercury Self-Alert Monitor Settings**.
5. In the Mercury Business Availability Center Machine View table, select the check box of the machine whose components you want to reconfigure.
6. Click **Save Settings**.

Creating a Baseline for the Mercury Self-Alert Monitor Group

Following setup, SiteScope begins monitoring the Mercury Business Availability Center machines registered in the Mercury Business Availability Center Management database. You must now bring the Mercury Self-Alert Monitor group to the state where all monitors have an OK status, that is, the Self-Alert Monitor group icon in the SiteScope main view is green. In this way, you can create a reliable baseline against which you can compare subsequent monitor results.

Mercury Self-Alert Monitor Templates

The Self-Alert monitors check the Mercury Business Availability Center components, according to the definitions in the ***.mset** files, located in the **<SiteScope root directory>templates.sets.topazWatchdog** directory.

The Mercury Self-Alert Monitors monitors can be customized either by changing one of the monitor templates or by adding monitor templates, and assigning them to a specific Mercury Business Availability Center service.

The file which maps monitor templates for each Mercury Business Availability Center service is named **defaultMercury Application ManagementWatchdogMonitorSets.config**, and is located in the **<SiteScope root directory>\classes** directory. This file is copied to the **<SiteScope root directory>templates.sets.topazWatchdog** directory with the name **topazWatchdogMonitorSets.config** the first time that SiteScope starts.

The following is an example of an entry in this file:

```
_descriptionForUi=Alert Server
_topazHostTypeMask=128
_monitorSets_Windows=Common.mset,Mercury Application
ManagementSupervisor.mset,AlertServer.mset
_monitorSets_Unix=CommonUNIX.mset,Mercury Application
ManagementSupervisorUNIX.mset,AlertServerUNIX.mset
```

where:

_descriptionForUi is a description of the specific Mercury Business Availability Center service

_topazHostTypeMask is an internal ID of the specific Mercury Business Availability Center service. You must not change this value.

_monitorSets_Windows is a comma separated list of Monitor Set files which are associated with this Mercury Business Availability Center service on a Windows platform (the specified monitor sets must reside in the **<SiteScope root directory>templates.sets.topazWatchdog** directory).

_monitorSets_UNIX is a comma separated list of monitor set files that are associated with this Mercury Business Availability Center service on a UNIX platform (the specified monitor sets must reside in the **<SiteScope root directory>templates.sets.topazWatchdog** directory).

Important: Before making any direct modifications, make a complete backup of the SiteScope folders. After making any modifications, test that your monitors, alerts, and reports are functioning correctly before returning them to a production environment.

Configuring Monitor Solution Templates

You can replicate monitors across multiple servers or locations using the SiteScope solution template functionality. You work with Mercury Self-Alert Monitor templates in the same way as you work with SiteScope monitor solution templates.

To enable working with Mercury Self-Alert Monitor monitor sets:

1 In the **<SiteScope root directory>templates.sets.topazWatchdog** directory, choose the templates with which you want to work. Monitor template files have the **.mset** extension.

Each template includes a list of variables, their descriptions and values, and the monitors that are configured by the template. For example, the Mercury Business Availability Center Centers Server template includes the variable $TOPAZ_HOST_NAME$. Its description is **Server_to_monitor** (the underscores do not appear in the SiteScope page.

Copy the template **.mset** files to the **<SiteScope root directory>templates.sets** directory.

2 To use the templates, click the **Mercury Self-Alert Monitor** group in the SiteScope main view, then click **Add Monitor Set**. The Add Monitor Set to Group page opens. Select the monitor template that you want to configure, and click **Configure**.

3 Click **Submit** to save the new monitor template.

Mercury Self-Alert Monitor Troubleshooting

The following table describes a number of conditions that may cause errors to be reported after you have set up the Mercury Self-Alert Monitor group. The Resolution column lists actions you can take to correct the error.

Problem Description	Resolution
SiteScope does not have the appropriate permissions to access the machine on which the Mercury Business Availability Center Admin Server is installed.	If this is the case, SiteScope shows error statuses for all monitors that are reporting on the operating system of the Mercury Business Availability Center machine. Check the user access permissions that have been granted to the SiteScope account on the remote server. SiteScope requires remote registry permissions to be able to monitor server statistics. Try connecting to the remote machine using Perfmon.
A machine is down for maintenance.	You can temporarily remove the machine from the Mercury Business Availability Center Self-Alert Monitor Settings page.
A Business Process Monitor is not sending data.	Check why the Business Process Monitor is not working. Possible causes: the Business Process Monitor machine is down or a process is stuck; there are network problems so the Business Process Monitor cannot connect to the Mercury Business Availability Center Core Server; the Mercury Business Availability Center loaders are failing to insert the data into the profile database; the Mercury Business Availability Center management database is down; the profile database is down.

The Last Reported Data Time monitor has an error among its components.	The Last Reported Data Time monitor is different from other monitors because it checks a complete, round-trip process, and not one specific component of a process. It may be that at some point in the round trip a problem was found: try and isolate the problem by looking at a Mercury Business Availability Center Core Server monitor.
The monitor name: **File-Age <sample type> Buffers Read** on **$TOPAZ_HOST_NAME$** indicates an error. **Note: <sample type>** can be one of the following: Transaction, SiteScope, WebTrace, EMS, J2EE.	This problem may indicate that the Mercury Business Availability Center loaders are failing to insert the data collection samples into the profile database. SiteScope checks the time that the **Read** directory in each loader was last modified, and uses predefined thresholds for this monitor: If the time since the loader was last modified is more than 4 minutes, SiteScope issues a warning. If the time since the loader was last modified is more than 8 minutes, SiteScope issues an error. If you know that the interval at which the relevant data collectors report data to Mercury Business Availability Center is higher than these thresholds, you should change the threshold for warnings and errors in these monitors.

Troubleshooting Directory and Log File Errors

If one or all Directory monitors indicate a "directory not found" error, and all log file monitors indicate an "unable to read log file" error. These errors can happen when you monitor a Mercury Business Availability Center system running on Windows operating systems. The cause of this type of error is likely because the Mercury Self-Alert Monitor assumes that the Mercury Business Availability Center installation path is: C:\MercuryAM.

Note: When making any of the changes described here, you should make a backup of the files that are to be modified.

Note: After making any of the changes described here, you must stop and restart the SiteScope service for the changes to take effect.

To resolve this problem, do one (or more) of the following:

Modify the Templates

Use the following steps to modify the templates.

To modify the templates:

1. Edit the Mercury Self-Alert Monitor monitor templates in the **<SiteScope root directory>templates.sets.topazWatchdog** directory, and replace the $TOPAZ_FOLDER$ string with the location on the local disk where Mercury Business Availability Center is installed. For example, if Mercury Business Availability Center is installed on volume D, change $TOPAZ_FOLDER$ to D$\Topaz.

   If the Mercury Business Availability Center folder is shared by the name MercuryAM, change $TOPAZ_FOLDER$ to be MercuryAM.

2. Save the changes to the file.

3. Update the Self-Alert Monitor using the following steps:

   a Navigate to the Mercury Self-Alert Monitor Settings page.

   b Disable machines for which the wrong directory path is used.

   c Save the changes.

   d Re-enable the machines.

Modify the Configuration File

Use the following steps to modify the configuration file.

To modify the configuration file:

1. Open **<SiteScope root directory>\groups\watchdog.config**, and change the value of the _twdTopazFolder parameter.
   For example, you can set this parameter to D$:\MercuryAM by changing the line
   _twdTopazFolder=C$ \MercuryAM
   to:
   _twdTopazFolder=D$ \MercuryAM.
   You can set this parameter a network drive share alias name by changing the line
   _twdTopazFolder=C$ \MercuryAM
   to:
   _twdTopazFolder=<NETWORK SHARE ALIAS>.
2. Save the changes to the file.
3. Update the Self-Alert Monitor using the following steps:

Note: If you clear the Mercury Self-Alert Monitor settings, the _twdTopazFolder parameter is reset to C$ \Topaz.

---

   a. Navigate to the Mercury Self-Alert Monitor Settings page.
   b. Disable machines for which the wrong directory path is used.
   c. Save the changes.
   d. Re-enable the machines.

Edit the Individual Monitors

Edit each problematic monitor, and change its directory path or the log file pathname attributes to the correct directory or file path.

After making any changes, stop and restart SiteScope.

More Troubleshooting Issues

The following table lists a number of other conditions that may occur when using the Mercury Self-Alert Monitor with Mercury Business Availability Center.

Problem	Solution(s)
In a Windows 2000 installation, drive letters are replaced by HarddiskVolume1, HarddiskVolume2, and so forth.	For the solution, refer to: http://support.microsoft.com/support/kb/articles/Q274/3/11.asp. (Microsoft Knowledge Base article number Q274311)
In a Windows 2000 or 2003 installation, no disks are monitored by SiteScope.	This occurs when a Windows 2000 installation has disk monitoring disabled by default. To enable disk monitoring, open a command line window, and enter the command diskperf -y. After restarting the computer, the disks are added to SiteScope.
If the Mercury Business Availability Center Admin server is installed on Apache, on a machine that automatically runs Microsoft IIS, SiteScope may not measure the correct process, and performance may be impeded.	Make sure that only the Web server that Mercury Business Availability Center uses is running. Some systems, for example, Windows 2000, have IIS automatically installed and running. Therefore, if Mercury Business Availability Center is installed on Apache, on a Windows 2000 server, both IIS and Apache will be running, which slows down performance and scalability. Stop the IIS service and disable it from running automatically. This will ensure that the machine runs faster, and that SiteScope measures the correct process.

If a network drive to a server has been mapped with non-administrative credentials, you cannot open a new authenticated network connection with administrative permissions, or change the existing one.	This is a Windows networking limitation. The solution is not to disconnect the mapped drive, as the connection will remain alive. The problem also occurs if you run Terminal services to a machine or just explore it with Explorer. It can be destroyed only after a reboot of the SiteScope machine. If you are still not able to monitor a server even if you know the administrator user name and password, you should run netstat -a, to see if there is an active (established) connection to that machine.
SiteScope cannot connect to a remote Windows server.	If a connection cannot be made, check the user access permissions that have been granted to the SiteScope account on the remote server. SiteScope requires remote registry permissions to be able to monitor server statistics. Try connecting to the remote machine using Perfmon.
SiteScope is not allowed to use the permissions of a full administrator account.	This may be for security reasons. SiteScope can be granted restricted monitoring access by editing certain Registry Keys. See the Enabling Non-Admin Users to Remotely Monitor with PERFMON support note on the Microsoft support site for more information.
SiteScope cannot monitor a stand-alone server, or one that is part of a domain already visible to the SiteScope server.	Try entering the machine name followed by a slash and the server name in the Login entry box. For example, type cats/administrator
SiteScope does not monitor the load balancer machine.	SiteScope cannot display data about load balancer machines because they are not Mercury Business Availability Center hosts. You can set up a standard SiteScope monitor to monitor the load balancer machines, and to send an alert when the load balancer is in error. For details, see "Working with SiteScope Monitors" in *Configuring SiteScope Monitors*.

Monitors are returning errors on specific machines.	Check whether the machine has been added to the Remote Windows Servers or Remote UNIX Servers list. For details, see "Defining Permissions for NT Servers" and "Defining Permissions for UNIX Servers". Check whether remoteRegistryService is running on the Mercury Business Availability Center machine. A Microsoft Windows problem causes the registry service RemoteRegistryService to hold too many handles that are not released. Every time SiteScope logs in to the Mercury Business Availability Center server, another handle is added. To see how many handles are being held by a process, display the **Processes** tab in the Windows Task Manager, and look for the Handles column. (If the Handles column does not appear, choose **View** > **Select Columns** > **Handles**.) To release handles, restart the service, either manually: net stop "remote registry" net start "remote registry" or with a script that is set to run, for example, every six hours (but can depend on the specific setup), by using Windows Task Scheduler (**Scheduled Tasks** in Explorer). Example of the script: at 12:00 /every:Su,M,T,W,TH,F,S net stop RemoteRegistry at 12:01 /every:Su,M,T,W,TH,F,S net start RemoteRegistry at 18:00 /every:Su,M,T,W,TH,F,S net stop RemoteRegistry at 18:01 /every:Su,M,T,W,TH,F,S net start RemoteRegistry at 00:00 /every:Su,M,T,W,TH,F,S net stop RemoteRegistry at 00:01 /every:Su,M,T,W,TH,F,S net start RemoteRegistry at 06:00 /every:Su,M,T,W,TH,F,S net stop RemoteRegistry at 06:01 /every:Su,M,T,W,TH,F,S net start RemoteRegistry

	Sometimes counters for perfmon objects are disabled on the Mercury Business Availability Center machine (for example, for the Process object). To monitor such a machine, you must enable these objects. You can do this either with the help of the Windows Resources Kit, or via the registry. With the Windows Resources Kit, in the Extensible Counter Kit dialogue box, check that the **Performance Counters Enabled** check box is selected, for the PerfProc and PerfOS objects. Using the registry, check that the following files are set to 0: HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\PerfProc\ Performance]"Disable Performance Counters"= dword:00000000 and HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\PerfOS\ Performance]"Disable Performance Counters"= dword:00000000

SiteScope sends false alerts.	This is an integration issue, with two causes: SiteScope has been disconnected from Mercury Business Availability Center, and alerts are sent several minutes after the disconnection. To prevent this, clear the check box next to the SiteScope machines, or use the Data Collector Maintenance page, accessed from **Admin** > **Platform** > **Data Collection** > **Data Collector Maintenance** in Mercury Business Availability Center, to remove the SiteScope no longer in use. SiteScope has been moved from one profile to another, and alerts are sent during the period when SiteScope is in downtime. To prevent false alerts, delete the old SiteScope profile (preferred), or disable the alerts for this host.
The same host appears twice in the SiteScope main panel.	During probe definition, the probe's location is registered by its relationship to the location of the Business Process Monitor host that is running the probe. If the definition of this Business Process Monitor is changed, and if its new location is different from the previous one, the new registration and location for the probe is added to the Host table in the Mercury Business Availability Center management database. The result is that the table includes two probe hosts with the same name but with different locations. This causes SiteScope to display the probe host twice in the main panel.

13

Host Last Connection Time Monitor

The Mercury Business Availability Center Host Last Connection Time Monitor checks the last time a Business Process Monitor, SiteScope or Client Monitor Agent contacted the Mercury Business Availability Center Server.

This chapter describes:	On page:
Understanding the Host Last Connection Time Monitor	135
Configuring the Host Last Connection Time Monitor	136

Understanding the Host Last Connection Time Monitor

Host Last Connection Time Monitor part of the Mercury Self-Alert Monitor solution. The Mercury Self-Alert Monitor automatically configures this monitor type for a Business Process Monitor, SiteScope or Client Monitor. For details, see "Mercury Self-Alert Monitor" on page 115.

Note: This monitor cannot be configured independently or from the regular SiteScope user interface. It is deployed only when the Mercury Self-Alert Monitor is deployed from the SiteScope classic interface. Only then does the monitor appear within the Mercury Self-Alert Monitor group.

The Business Process Monitor is scheduled to connect to Mercury Business Availability Center every two minutes. If the last connection was more than four minutes ago, Mercury Self-Alert Monitor sets a warning status for this monitor. If the last connection was more than six minutes ago, Mercury Self-Alert Monitor sets an error status.

SiteScope is scheduled to connect to Mercury Business Availability Center every 24 hours. If the last connection was made 24 hours and 10 minutes ago, Mercury Self-Alert Monitor sets a warning status for this monitor. If the last connection was 25 hours ago, Mercury Self-Alert Monitor sets an error status.

For Client Monitor Agents, Mercury Self-Alert Monitor always sets an OK status, since Client Monitor Agents are located on machines that may not be open all the time, or operating all the time.

You can change the Error and Warning times, if you know that a specific Agent connects to Business Availability Center at a different frequency than the default one.

Configuring the Host Last Connection Time Monitor

The Host Last Connection Time monitor cannot be added to a SiteScope monitor group container in the monitor tree. The monitor is automatically configured as a result of deploying Mercury Self-Alert monitoring from the SiteScope classic interface. Once Mercury Self-Alert monitoring is deployed, the Host Last Connection Timeis appears in a Mercury Self-Alert Monitor group in the tree. You can modify the properties of this monitor using the Properties tab. The following sections list the settings for the Host Last Connection Time Monitor.

Main Settings for the Host Last Connection Time Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the system, how often this Host Last Connection Time Monitor instance should be run, and the text name used for this monitor instance. See “Common Monitor Settings” in the chapter “Working with SiteScope Monitors” for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Host Last Connection Time monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Host Last Connection Time Monitor should system check the system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Host Location

The location from which this agent is reporting. The Mercury Self-Alert Monitor automatically knows the location of this agent according to the agent registration details in Business Availability Center.

Host ID

Enter the host ID of this agent in Mercury Business Availability Center. The Mercury Self-Alert Monitor automatically knows the Host ID of this agent according to the agent registration details in Business Availability Center.

Advanced Settings for the Host Last Connection Time Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Host Last Connection Time Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- Enable all associated alerts
- Disable all associated alerts for the next time period
- Disable all associated alerts on a one time schedule
- Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Host Last Connection Time Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

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

14

Host Last Reported Data Time Monitor

The Host Last Reported Data Time Monitor checks the time stamp of the last data that reached Mercury Business Availability Center from a specific Business Process Monitor, SiteScope, or Client Monitor.

This chapter describes:	On page:
Understanding the Host Last Reported Data Time Monitor	141
Configuring the Host Last Reported Data Time Monitor	142

Understanding the Host Last Reported Data Time Monitor

The Host Last Reported Data Time Monitor is part of the Mercury Self-Alert Monitor solution. The Mercury Self-Alert Monitor automatically configures this monitor type for the different data collectors running in Mercury Business Availability Center. This monitor type is different from other monitors, because it checks a complete, round-trip process, and not one specific component of a process. For details, see "Mercury Self-Alert Monitor" on page 115.

Note: This monitor cannot be configured independently or from the regular SiteScope user interface. It is deployed only when the Mercury Self-Alert Monitor is deployed from the SiteScope classic interface. Only then does the monitor appear within the Mercury Self-Alert Monitor group.

The OK status means that the monitored data collector is reporting data to Mercury Business Availability Center server. The data is then made available to the various Mercury Business Availability Center applications.

An error status means that somewhere in the round trip, a problem was found. You use other monitors in the Mercury Self-Alert Monitor group to identify where the problem might be.

When Mercury Self-Alert Monitor solution automatically creates this monitor to check the Business Process Monitor, it sets a warning status if the time period since the last reported data is longer than the maximum amount of time that the specific Business Process Monitor has been configured to report to Mercury Business Availability Center. Mercury Self-Alert Monitor sets an error status if the time period since the last reported data is longer than twice the same amount of time.

As the Mercury Self-Alert Monitor group can retrieve the frequency at which the Business Process Monitor checks processes, the last reported data time for this monitor is calculated according to this specific frequency. This is not the case with SiteScope, which is why it is monitored at a predefined threshold.

When the Mercury Self-Alert Monitor automatically creates this monitor for Client Monitors, this monitor always has an OK status, since it does not check the status of the data collector when reporting its activities. This is because Client Monitors are located on machines that may not be open all the time, or operated all the time.

Configuring the Host Last Reported Data Time Monitor

The Host Last Reported Data Time monitor cannot be added to a SiteScope monitor group container in the monitor tree. The monitor is automatically configured as a result of deploying Mercury Self-Alert monitoring from the SiteScope classic interface. Once Mercury Self-Alert monitoring is deployed, the Host Last Reported Data Timeis appears in a Mercury Self-Alert Monitor group in the tree. You can modify the properties of this monitor using the Properties tab. The following sections list the settings for the Host Last Reported Data Time Monitor.

Main Settings for the Host Last Reported Data Time Monitor

You use the Main Settings section to specify how SiteScope should connect to or check the system, how often this Host Last Reported Data Time Monitor instance should be run, and the text name used for this monitor instance. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information. Complete the entries in the Main Settings section as described below.

Name

Enter a text name for this Host Last Reported Data Time monitor instance. This text is displayed in the Monitor Administration interface and other places in the SiteScope interface.

Frequency

Select how often the Host Last Reported Data Time Monitor should system check the system. Use the drop-down list to the right of the text box to specify a frequency interval in increments of seconds, minutes, hours, or days. The update interval must be a minimum of 15 seconds or longer.

Host Location

The location from which this agent is reporting. Note that Mercury Self-Alert Monitor automatically knows the location of this agent according to the agent registration details in Business Availability Center.

Host ID

Enter the host ID of this agent in Mercury Business Availability Center. Note that Mercury Self-Alert Monitor automatically knows the Host ID of this agent according to the agent registration details in Mercury Business Availability Center.

Advanced Settings for the Host Last Reported Data Time Monitor

The Advanced Settings section presents a number of ways to customize the behavior of the Host Last Reported Data Time Monitor and its display in the product interface. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information about settings that are

common to all monitor types. Complete the entries as needed and click the **Ok** button to save the settings.

Show Run Results On Update

Select this option to have SiteScope display the results of the monitor run in a dialogue box whenever a change is made to the configuration settings. When unchecked, no monitor run dialogue will be displayed when the monitor configuration is updated. For both cases, the updated run results are displayed in the applicable dashboard views for the monitor.

Verify Error

Check this box if you want SiteScope to automatically run this monitor again if it detects an error. It is recommended that you not use this option as it can cause a number of problems in large monitoring environments. See "Common Monitor Settings" in the chapter "Working with SiteScope Monitors" for more information.

Error Frequency

You use this option to set a new monitoring interval for monitors that have registered an error condition. For example, you may want to run the monitor every 10 minutes normally, but as often as every 2 minutes if an error has been detected.

Note: Using this option to increase the run frequency of a monitor will also effect the number of alerts generated by this monitor.

Monitor Schedule

By default, SiteScope monitors are enabled every day of the week. To have the monitor run only during a specific time schedule, select a schedule profile from the drop-down menu.

Depends On

To make the running of this monitor dependent on the status of another monitor, expand the node in the SiteScope tree containing the monitor to which to you want to create dependence, and select the check box next to

the appropriate monitor. You can create dependence on multiple monitors by selecting more than one monitor in the tree. To remove dependence on a monitor, clear the appropriate check box.

Depends Condition

If you choose to make the running of this monitor dependent on the status of another monitor, select the status condition that the monitor selected in the **Depends On** field should have for the current monitor to run normally.

Monitor Description

Enter additional information to describe this monitor. The description text will appear on the Content panel for the group to which the monitor belongs.

Report Description

Enter an optional description displayed on report bar charts and graphs in Management Reports.

Enable/Disable Monitor Settings

The Enable/Disable Monitor settings are used to interrupt the actions performed by an individual monitor or group of monitors. The options in this section are:

- Enable Monitor
- Disable Monitor indefinitely
- Disable Monitor for the next time period
- Disable Monitor on a one time schedule
- Disable Description

For details, see "Disabling and Enabling Monitors" in *Managing SiteScope*.

Enable/Disable Alerts Settings

The Enable/Disable Alerts settings are used to disable or enable any alert actions that may be triggered by an individual monitor or group of monitors. The options in this section are:

- ➤ Enable all associated alerts
- ➤ Disable all associated alerts for the next time period
- ➤ Disable all associated alerts on a one time schedule
- ➤ Disable Description

For details, see "Disable or Enable Monitors Alerts" in *Configuring SiteScope Alerts*.

Setting Monitor Status Thresholds

You use the Threshold Settings section to set logic conditions that determine the reported status of each monitor instance. The status result is based on the results or measurements returned by the monitor action on the target system. See "Common Monitor Settings" in the section "Working with SiteScope Monitors" for more information on working with status thresholds.

You can set up to ten status thresholds criteria for each status condition per monitor instance. By default, only one threshold is displayed when you first configure the monitor.

Each status threshold consists of a measurement parameter, a logic comparison operation, and a measurement threshold value that you may specify. You may use the default status thresholds defined for the Host Last Reported Data Time or use the following steps to change the monitor status thresholds for this monitor instance.

To edit monitor status thresholds:

1. Use the first drop-down menu for the **Error if** setting to select the measurement parameter which you want to use to determine the status of this monitor instance.
2. Use the second drop-down menu to select the comparison operator(s) that will define the status threshold.
3. Enter a value applicable to the measurement parameter in the third text box.
4. To add another threshold setting, click the **New Error If** button and repeat the steps above.

5 Use these steps to create **Warning if** and **Good if** settings, selecting the appropriate parameters and comparison operators, and entering corresponding values in the fields provided.

Configuration Item Attachment Settings

Optionally, expand the Configuration Item Attachment Settings area to attach a CI to this monitor. For details, see "Configuration Items and Monitor Objects" in *Working with Monitor Administration*.

Note: The Configuration Item Attachment Settings are available only when adding a SiteScope monitor to Monitor Administration and cannot be set while editing a monitor.

Mercury BAC Logging

You use the Mercury BAC Logging section to control what data from the Host Last Reported Data Time Monitor will be forwarded to the Mercury Business Availability Center database. You use the radio buttons to select one of the following options:

- Do not report to Mercury Business Availability Center
- Report everything (all monitors and all measurements)
- Report monitor level data (no measurements)
- Report monitor level data and measurements with thresholds
- Report status changes (no measurements)

For details, see "Common Monitor Settings" in the chapter Chapter 2, "Working with SiteScope Monitors."

Category Settings

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

Index

A

accounts
  SiteScope administrator e-mail - Windows 44

C

connecting to SiteScope 34
Copy Monitors utility 55
  limitations 56
  requirements 56
  URL to access 58
  usage 55
Copy Monitors, requirements for using 54
copying configuration data 57
Core Server
  changing in SiteScope 95

F

First-time Setup page 35, 36, 52

H

Host Last Connection Time Monitor 135
Host Last Reported Data Time Monitor 141

I

installation
  account permissions on UNIX 16
  copying configurations from other SiteScopes 55
  do not run SiteScope as root 16
  on Solaris or Linux 15
  on Windows 41
  preparing for on Solaris or Linux 15
installing SiteScope
  creating an installation template 33
  using console mode 26
  using installation template 34
  using the installation executable 17

L

license
  new for SiteScope 8.0 37
Linux
  installing SiteScope for 15
  preparation for SiteScope installation 15
  requirements for SiteScope on 7
log files
  SiteScope 12

M

Mercury Application Management Host Last Connection Time
  about 135
Mercury Application Management Host Last Connection Time Monitor 135
  advanced settings 137
  configuring 136
Mercury Application Management Host Last Reported Data Time Monitor 141
  about 141
  advanced settings 143
  configuring 142
Mercury Business Availability Center
  changing Core Server reporting 95
  integration with 85
  registering SiteScope to 90
  SiteScope integration with 86

troubleshooting data reporting to 102
using SSL for communication to 99
Mercury Managed Services
integrating SiteScope with 103
Mercury Self-Alert Monitor 115
creating a baseline 122
disabling 120
reconfiguring a component 121
setting up 118
templates 122
troubleshooting 125
updating target path 121
working with 117
Mercury SiteSeer
integrating SiteScope with 109
settings for integration 111
monitors
copying configurations 55

P

ports
conflicts with other applications 32

S

security
access control lists 72
hardening SiteScope 71
SiteScope account permissions 16
using SSL 73
SiteScope
administrator e-mail 21, 44
before upgrading 10
configuring for SSL 78
controlling access by IP 72
copying monitors from another installation 53
First-time Setup - Getting Started page 38, 53
First-time Setup Screen 35, 52
hardening 71
installation, before you begin 5
installation, selecting install folder 46
logs directory contents 12
Open SiteScope page 49
recommended server configurations for installation 7
server sizing considerations for installation 9
system files for upgrade 11
system requirements 5
technical support registration 13
uninstall 61
using SSL 73
SiteScopes
sizing multiple installations 8
sizing
considerations for SiteScope 9
sizing multiple SiteScopes 8
Solaris
installing SiteScope for 15
preparation for SiteScope installation 15
requirements for SiteScope on 6
SSL
configuring in SiteScope 73
configuring SiteScope to use 78
importing a CA certificate 76
keytool utility 74
to access SiteScope 72
using a CA certificate 74
using self-signed certificates 77
system requirements
for SiteScope on Linux 7
for SiteScope on Solaris 6
for SiteScope on Windows 6
SiteScope installation 5
SiteScope recommended server configurations 7

T

technical support
registering for SiteScope 13

U

uninstall SiteScope 61
    on Solaris or Linux 63
    on Windows 61
    temporary install files on UNIX 64
    temporary install files on Windows 61
UNIX
    to uninstall SiteScope 63
upgrade
    copying configurations 55
    copying monitors from another SiteScope installation 53
    key SiteScope files 11
upgrading SiteScope 10

W

Windows
    requirements for SiteScope on 6
Windows 2000
    installing SiteScope for 41
    to uninstall SiteScope 61